Novell Identity Manager Driver for Active Directory*

3.1

www.novell.com

实施指南

2006 年 4 月 28 日



Novell®

法律声明

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

联机文档：要访问本产品和其它 Novell 产品的联机文档或获取产品的更新，访问下列网址：
www.novell.com/documentation。

Novell 商标

第三方资料

目录

关于本指南

本指南说明如何安装、配置和管理 Identity Manager Driver for Active Directory。

读者

本指南适用于 Active Directory 管理员、 Novell® eDirectory™ 管理员及其他实施 NT 域的 Identity Manager 驱动程序的人员。

反馈

我们希望听到您对于本手册和本产品包含的其它文档的意见和建议。请使用联机文档的每一页底端的 《用户意见》功能，或进入 www.novell.com/documentation/feedback.html，然后在该网页中输入您的意见。

文档更新

有关本文档的最新版本，请访问驱动程序文档万维网站点 (http://www.novell.com/documentation/lg/dirxmldrivers)。

其它文档

有关使用 Identity Manager 及其它 Identity Manager 驱动程序的文档，请参见 Identity Manager 文档万维网站点 (http://www.novell.com/documentation/lg/dirxml20)。

文档约定

在 Novell 文档中，大于号 (>) 用于分隔同一步骤中的各项操作，以及交叉参照路径中的各个项目。

商标符号 （® 、 ™ 等）表示 Novell® 商标。星号 (*) 表示第三方商标。

概述 1

1.1 主要术语

1.1.1 Identity Manager

Novell® Identity Manager 是一种服务，它可以使用一组可靠的可配置策略来同步一组已连接系统中的服务器之间的数据。Identity Manager 使用 Identity Vault 储存共享的信息，并使用 Metadirectory 引擎对 Vault 或已连接系统中发生更改的信息进行基于策略的管理。Identity Manager 在 Identity Vault 和 Metadirectory 引擎所在的服务器中运行。

1.1.2 已连接系统

已连接系统是指可通过驱动程序与 Identity Manager 共享数据的任何系统。Active Directory 就是一种已连接系统。

1.1.3 Identity Vault

Identity Vault 是 eDirectory™ 维护的永久数据库， Identity Manager 使用它来保存与已连接系统同步的数据。可以狭义地将 Vault 看作 Identity Manager 的私用数据储存，也可以广义地将它看作可保存企业级数据的 Metadirectory。Vault 中的数据可用于受 eDirectory 支持的任何协议，包括 NCP・ – onsoleOne® 和 iManager 等实用程序使用的传统协议）、 LDAP 和 DSML。

由于 Vault 由 eDirectory 维护，因此，可通过将现有的目录树用作 Vault，将 Identity Manager 方便地集成到公司目录基础结构。

1.1.4 Metadirectory 引擎

Metadirectory 引擎是实现事件管理和 Identity Manager 策略的核心服务器。该引擎在 eDirectory 中的 Java* 虚拟机上运行。

1.1.5 Active Directory 驱动程序

驱动程序可为已连接系统实现数据共享策略。可通过使用 iManager 定义过滤器和策略来控制驱动程序的操作。对于 Active Directory，驱动程序可实现单个域的策略。

1.1.6 驱动程序 Shim

驱动程序 Shim 是驱动程序的组件，它可以将基于 XML 的 Identity Manager 命令和事件语言 (XDS) 转换为与已连接系统交互时所需的协议和 API 调用。运行输出转换后，将调用 Shim 对已连接系统执行命令。命令通常在 《订购者》通道上生成，但也可以在 《发布者》通道上通过命令写回生成。

Shim 还可以针对输入转换策略在已连接系统上生成事件。可以在 Java 类中实现驱动程序 Shim，或者将驱动程序 Shim 作为本机 Windows DLL 文件来实现。Active Directory 的 Shim 为 ADDriver.dll。

ADDriver.dll 被作为本机 Windows DLL 文件来实现。ADDriver 使用若干个不同的 Windows API 来与 Active Directory 集成。通常这些 API 需要某种类型的登录和鉴定才能成功。同时，API 可能要求登录帐户在 Active Directory 中以及执行 ADDriver.dll 的计算机中具有某些权限和特权。

如果使用远程装载程序， ADDriver.dll 将在运行了远程装载程序的服务器上执行。否则，它将在运行了 Metadirectory 引擎的服务器上执行。

1.1.7 远程装载程序

远程装载程序能使驱动程序 Shim 在 Metadirectory 引擎以外执行 （有可能在不同的计算机上远程执行）。通常，当 Identity Manager 服务器无法满足驱动程序 Shim 的要求时，将使用远程装载程序。例如，如果 Metadirectory 引擎在 Linux* 上运行，则可以在 Windows 服务器上使用远程装载程序来执行 Active Directory 驱动程序 Shim。

远程装载程序是一种服务，它可以执行驱动程序 Shim，并可以在 Shim 和 Metadirectory 引擎之间传递信息。如果使用远程装载程序，则需要在运行了远程装载程序的服务器上 （而不是在运行了 Metadirectory 引擎的服务器上）安装驱动程序 Shim。可以选择使用 SSL 来加密 Metadirectory 引擎和远程装载程序之间的连接。

如果将远程装载程序与 Active Directory 驱动程序 Shim 一起使用，则存在两种网络连接：

- 域控制器和远程装载程序之间
- Active Directory 和 Active Directory 驱动程序 Shim 之间

1.2 新增功能

- “驱动程序功能”在第 6 页
- “Identity Manager 功能”在第 7 页

1.2.1 驱动程序功能

- 平台登录是一个驱动程序 Shim 配置参数。它可为 Shim 启用本地登录。启用本地登录后，《订购者》通道口令设置和口令修改将使用不需要 SSL 加密 LDAP 会话的平台口令管理 API。

使用 CDOEXM 的 Exchange 操作将使用鉴定和授权的线程身份来减少 LDAP 通道以外的操作失败的可能性。有关详细信息，请参考第 4 章 “配置 Active Directory 驱动程序”在第 31 页 。

- 将更新驱动程序 Shim 配置参数。驱动程序参数使用灵活提示，这样可以更好地对参数分类，以及更好地控制置于参数中的值。有一个下拉列表可以控制限制到一组已知值的参数，同时会检查需要整数值的参数是否存在无效字符。
- 将添加两个驱动程序 Shim 配置参数，用于控制 Microsoft Exchange 邮箱的移动和删除。在启用了 CDOEXM 和 Exchange 邮箱移动的情况下，如果对已经保留了 Exchange 邮箱的用户对象设置 homeMDB 特性值，将使该邮箱移至新的 Exchange 讯息数据库。Shim 只支持域内移动：承载新的讯息数据库的 Exchange 服务器必须在 Shim 管理的同一域中。
- 通过用户应用程序或策略增强对基于职能的权利的支持。请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Creating and Using Entitlements》（创建和使用权利）。
- 驱动程序 Shim 包括对扩展查询 (query-ex) 的支持。扩展查询能使 LDAP 搜索的结果分页。Shim 可通过此功能将较大的数据集从 Active Directory 迁移到 Identity Vault。有关从 Active Directory 进行迁移的更多信息，请参见第 8 章 “查错”在第 75 页 。

1.2.2 Identity Manager 功能

有关 Identity Manager 新功能的信息，请参见 《*Identity Manager 3.0 安装指南*》中的 《Identity Manager 3 有哪些新功能？》。

1.3 系统间的数据传送

本节说明数据如何在 Active Directory 和 Identity Vault 之间流动。

1.3.1 发布者通道和订购者通道

Active Directory 驱动程序支持 《订购者》和 《发布者》通道。

《发布者》通道的功能如下：

- 从域的 Active Directory 中读取事件，该域驻留在与驱动程序 Shim 连接的服务器上。
- 将该信息提交给 Identity Vault。

《订购者》通道的功能如下：

- 监视对 Identity Vault 对象的添加和修改操作。
- 更改 Active Directory 以反映这些更改。

驱动程序可以配置为同时允许 Active Directory 和 Identity Vault 更新特定的特性。在此配置中，特性值由最近的更改决定，例外的情况是受过滤器和合并权限控制的合并操作。

1.4 默认的驱动程序配置

Active Directory 驱动程序附带了一个称为 ActiveDirectory.xml 的默认配置文件。使用 Designer 或 iManager 导入该配置文件时，会创建一个驱动程序，带有适用于与 Active Directory 同步的一组规则和策略。如果您对驱动程序的要求不同于默认策略，则需要更改这些策略，以便达到所需策略的效果。请特别注意默认的匹配策略。您相信可用于匹配用户

的数据通常不同于默认值。策略本身带有注释，导入测试驱动程序后，在 Designer 或 iManager 上检查这些策略可以更好地了解它们的功能。

1.4.1 用户对象名称映射

通常， Identity Vault 的管理实用程序 （例如 iManager 和 ConsoleOne）对用户对象的命名方式，不同于 Microsoft* 管理控制台 (MMC) 的 《用户》和 《计算机》咬接模块对用户对象的命名方式。请确保您了解这些差别，以便能够正确实现所拥有的匹配策略和任何转换策略。

1.4.2 数据流

数据可以在 Active Directory 和 Identity Vault 之间流动。数据流受到为 Active Directory 驱动程序部署的策略的控制。

策略

策略可以控制 Active Directory 和 Identity Vault 之间的数据同步。

在配置驱动程序过程中，可以使用 Active Directory 配置文件选择用于影响默认策略以及为您创建的过滤器的多个选项。表 1-1 在第 8 页 列出了这些选项，同时说明了它们如何影响策略和所创建的过滤器：

表 *1-1* 数据流选项

选项	说明
	《配置数据流》可以建立初始的驱动程序过滤器，该过滤器可控制将要同步的类和特性。此选项的用途在于配置驱动程序，以便以最佳方式表示常规的数据流策略。导入后，可以更改该选项以反映特定的需求。 选择 《Bidirectional （双向）》可设置类和特性，以便同步 《发布者》和 《订购者》通道。Identity Vault 和 Active Directory 发生的更改会同时在两端进行反映。如果希望两端都成为授权的数据源，请使用此选项。 选择 《AD 到 Vault》可设置类和特性，以便只同步 《发布者》通道。Active Directory 发生的更改将在 Identity Vault 中反映，但 Identity Vault 发生的更改将被忽略。如果希望 Active Directory 成为授权的数据源，请使用此选项。 选择 《Vault 到 AD》可设置类和特性，以便只同步 《订购者》通道。Identity Vault 发生的更改将在 Active Directory 中反映，但 Active Directory 发生的更改将被忽略。如果希望 Vault 成为授权的数据源，请使用此选项。
	《发布者布局》控制在 Identity Vault 中的哪个位置创建对象。 选择 《镜像》可将对象放在 Identity Vault 的层次中，该层次与对象在 Active Directory 中所在的层次相同。 选择 《平面》可将所有对象放在配置过程中指定的 Identity Vault 基本树枝中。

选项	说明
	《订购者布局》控制如何将对象放在 Active Directory 中。 选择 《镜像》可将对象放在 Active Directory 的层次中，该层次与对象在 Identity Vault 中所在的层次相同。 选择 《平面》可将所有对象放在配置过程中指定的 Active Directory 基本树枝中。

表 1-2 在第 9 页 列出了默认的策略，并说明了在配置过程中，选项如何影响这些策略：

表 ***1-2*** 默认策略

策略	说明
创建	在镜像层次或平面层次中，必须定义全名，以便将 Active Directory 用户创建为 Identity Vault 用户。
匹配	在镜像层次中，匹配策略将尝试与位于层次中相同位置的对象匹配。 在平面层次中，匹配策略会尝试将用户与您在基本树枝中指定的具有相同全名的对象相匹配。
布局	在镜像层次中，布局策略会将所有对象放在一个层次中，该层次可镜像发送操作的数据储存的层次。 在平面层次中，布局策略会将所有对象放在指定的基本树枝中。

纲要映射

下列 Identity Vault 用户特性、组特性和组织单元特性将映射到 Active Directory 用户特性和组特性。

表中列出的映射为默认映射。可以重映射相同类型的特性。

表 ***1-3*** 为所有类映射的特性

eDirectory	Active Directory
CN	cn
Description	description
Facsimile Telephone Number	facsimiletelephoneNumber
Full name	displayName
Given Name	givenName
Initials	initials
Internet EMail Address	mail
L	physicalDeliveryOfficeName
Locality	locality

eDirectory	Active Directory
Login Disabled	dirxml-uACAccountDisabled
Login Expiration Time	accountExpires
Physical Delivery Office Name	l
Postal Code	PostalCode
Postal Office Box	postOfficeBox
S	st
SA	streetAddress
See Also	seeAlso
Surname	sn
Telephone Number	telephoneNumber
Title	title

eDirectory 中的 L 特性将映射到 Active Directory 中的 physicalDeliveryOfficeName 特性，eDirectory 中的 Physical Delivery Office Name 特性将映射到 Active Directory 中的 L 特性。由于名称相似的字段具有相同的值，因此以这种方式映射特性能使特性良好地配合 ConsoleOne 和 Microsoft 管理控制台。

表 ***1-4*** 为用户映射的特性

eDirectory	Active Directory
CN	userPrincipalName
DirXML-ADAliasName	sAMAccountName
Login Allowed Time Map	logonHours

表 ***1-5*** 映射的组织单元特性

eDirectory	Active Directory
Organizational Unit	organizationalUnit
OU	ou

名称映射策略

默认的配置包括两个名称映射策略，将它们一起使用有助于调解 Identity Vault 和 Active Directory 之间不同的命名策略。如果使用 Active Directory 的 《用户》和 《计算机》工具（Microsoft 管理控制台 （本文档中简写为 MMC）的一个咬接模块）创建一个用户，则可以看到该用户的全名被用作其对象名。用户对象的特性定义 Windows 2000 以前版本的登录名（又称 《NT 登录名》或 《sAMAccountName》）以及 Windows 2000 登录名 （又称《userPrincipalName》）。如果在 Identity Vault 中使用 iManager 或 ConsoleOne 创建用户，则对象名与用户登录名相同。

如果在 Active Directory 中使用 MMC 创建一些用户，以及在 Identity Vault 中或者在与 Identity Vault 同步的另一个已连接系统中创建其它对象，则对象可能在相对的控制台中不成对，因此可能根本无法在相对的系统中创建。

在使用 MMC 约定的 Active Directory 中，可以通过全名映射策略来管理对象。如果启用了该策略，则 Identity Vault 中的 Full Name 特性将与 Active Directory 中的对象名同步。

在使用 Identity Vault 约定的 Active Directory 中，可以通过 NT 登录名映射策略来管理对象。如果启用了该策略，则 Identity Vault 对象名可用于同步 Active Directory 中的对象名和 NT 登录名。Active Directory 与 Identity Vault 中的对象名相同， NT 登录名与 Identity Vault 登录名匹配。

如果同时启用了这两个策略，则 Active Directory 对象名就是 Identity Vault Full Name，但是 NT 登录名与 Identity Vault 登录名匹配。

如果同时禁用了这两个策略，则不执行特殊的映射。将会同步对象名，并且不提供用于创建 NT 登录名的特殊规则。由于 NT 登录名是 Active Directory 中的必备特性，因此在添加操作过程中，需要某种方法来生成一个此特性。NT 登录名 (sAMAccountName) 将映射到 Identity Vault 中的 DirMXL-ADAliassName，因此，既可以使用该特性来控制 Active Directory 中的 NT 登录名，也可以在订购者创建策略中构建自己的策略，以生成一个这样的特性。如果选择此策略，使用 MMC 创建的用户会将 MMC 生成的对象名用作 Identity Vault 中的对象名。登录 Vault 时，使用该名称可能会不方便。

Windows 2000 登录名策略

Windows 2000 登录名 （又称 userPrincipalName 或 UPN）在 Identity Vault 中没有直接的对等特性。UPN 看上去像电子邮件地址 (user@mycompany.com)，而事实上可能是用户的电子邮件名。在处理 UPN 时，务必记住的一点是该特性必须使用已针对域进行配置的域名 （@ 符号后面的部分），这样才能成功使用该特性。可以找出允许哪些域名，方法是使用 MMC 创建用户，然后在添加 UPN 时查看域名下拉框。

默认的配置提供了用于管理 userPrincipalName 的多个选项。如果设置了域，以便能够将用户的电子邮件地址用作 userPrincipalName，则可以使用用于跟踪用户的电子邮件地址的选项之一。可以将 userPrincipalName 接在 Identity Vault 或 Active Directory 的电子邮件地址之后，具体取决于哪一端为电子邮件授权。如果用户电子邮件地址不合适，则可以选择使用由用户登录名加上固定域名构建的 userPrincipalName。如果可以使用多个名称，请在导入以进行选择之后更新策略。如果这些选项都不合适，则可以禁用默认的策略，并写入自己的策略。

权利

使用权利可以更方便地将 Identity Manager 与 eDirectory 中的 Identity Manager 用户应用程序和基于职能的服务集成。如果使用用户应用程序，操作 （例如在 Active Directory 中供应帐户）将会延迟，直到完成了适当的批准。如果使用基于职能的服务，则会基于用户对象的特性 （而不是按常规的组成员资格）完成权限指派。这两个服务给 Identity Manager 带来了难题，因为从对象的特性来看，到底是已经予以批准还是用户与职能匹配，这一点并不明显。

权利是对 Identity Vault 中的对象记录此信息的标准化方法。从驱动程序的角度看，权利可以对 Active Directory 中的某个项目授权或取消授权。可以使用权利授予对 Active Directory 中某个帐户的权限、控制组成员资格，以及供应 Exchange 邮箱。驱动程序并不知道用户应用程序或基于职能的权利。它依赖用户应用程序服务器或权利驱动程序根据自己的规则对用户授予或取消权利。

仅当计划将用户应用程序或基于职能的权利与驱动程序一起使用时，才应该为驱动程序启用权利。

准备 Active Directory 2

本节包括：

2.1 Active Directory 前提条件

- ❑ 《*Identity Manager 3.0 安装指南*》的《安装 Identity Manager》一节中列出的 Novell® Identity Manager 3.0 及其前提条件。
- ❑ Windows 2003 Server，或者带有 Service Pack 2 或更高版本的 Windows 2000 Server。
- ❑ 运行 Active Directory (AD) 驱动程序的服务器上以及目标域控制器上的 Internet Explorer 5.5 或更高版本。
- ❑ Active Directory 域控制器 DNS 名称或 IP 地址，具体取决于鉴定方法。

此外，承载 Active Directory 驱动程序的服务器最好是 Active Directory 域的成员。供应 Exchange 邮箱和同步口令时需要这种条件。如果不需要这些功能，则只要使用简单 （简单联结）鉴定方式，服务器就可以是任何域的成员。要使用双向口令同步功能，必须选择《协商》鉴定选项。

2.2 计划安装

可以在域控制器或成员服务器上安装 Active Directory 驱动程序。开始安装驱动程序之前，请确定以下事项：

- 在哪个位置安装 Active Directory 驱动程序 Shim
- 如何解决安全问题

2.2.1 在哪个位置安装 Active Directory 驱动程序和 Shim

Active Directory 驱动程序 Shim 必须在一个受支持的 Windows 平台上运行。但是，不需要在此同一计算机上安装 Metadirectory 引擎。使用远程装载程序可以将引擎和驱动程序 Shim 分隔开来，这样便可以平衡不同计算机上的负载，或者适应公司的指令。

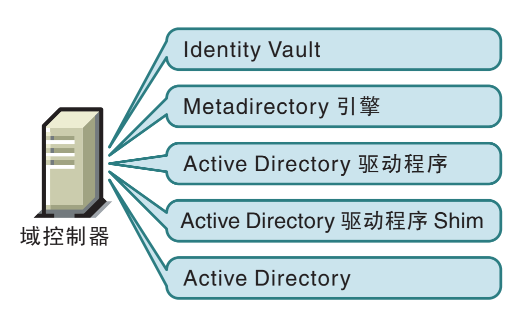
选择的安装方案将确定驱动程序 Shim 的安装方式。如果选择在 Identity Manager 所在的同一计算机 （Metadirectory 引擎和 Identity Vault 位于该计算机上）上安装驱动程序 Shim，则 Identity Manager 将直接调用驱动程序 Shim。如果选择在另一台计算机上安装驱动程序 Shim，则必须使用远程装载程序。

在每种方案中，将以相同的方式安装驱动程序本身。请参见第 4 章 "配置 Active Directory 驱动程序"在第 31 页 。

本地安装

单个 Windows 域控制器可以承载 Identity Vault、 Metadirectory 引擎和驱动程序。

图 **2-1** 方案 *1* - 所有组件在一台服务器上



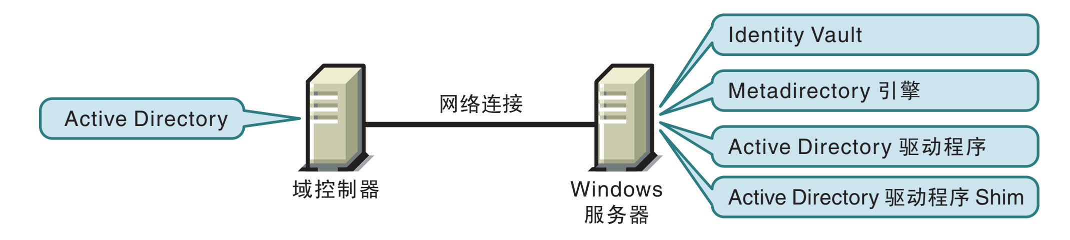
此配置非常适合希望节省硬件成本的组织。这也是性能最高的配置，因为 Identity Manager 和 Active Directory 之间不存在网络交通。

但是，在域控制器上承载 Identity Vault 和 Metadirectory 引擎会增加控制器的总体负载，并且会增大控制器出现故障的风险。由于域控制器在 Microsoft 联网中发挥着关键的作用，因此，与添加硬件的成本相比，许多组织更看重域鉴定的速度，以及域控制器故障相关的风险。

只在 **Windows** 服务器上远程安装

可通过 Active Directory 域控制器在独立的计算机上安装 Identity Vault、 Metadirectory 引擎和驱动程序。使用此配置则不需要在域控制器上安装任何 Identity Manager 软件。

图 **2-2** 方案 *2 - Active Directory* 和驱动程序 *Shim* 在不同的服务器上

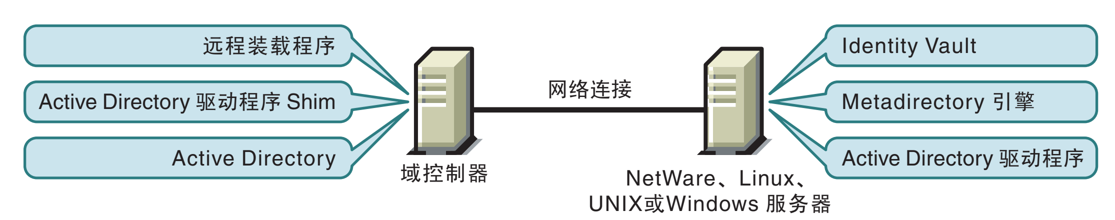


如果公司策略不允许在域控制器上运行驱动程序，则此配置很有吸引力。

在 **Windows** 和其它平台上远程安装

可以在 Active Directory 域控制器上安装远程装载程序和驱动程序 Shim，但需要在独立的服务器上安装 Identity Vault 和 Metadirectory 引擎。

图 **2-3** 方案 *3 - Active Directory*、远程装载程序和驱动程序 *Shim* 在一台服务器上



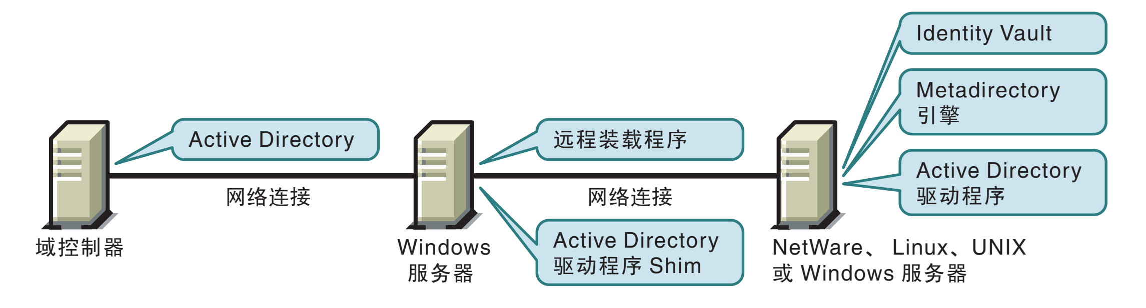
如果 Identity Vault 和 Metadirectory 引擎 (Identity Manager) 不是在一种受 Windows 支持的平台版本上安装的，则此配置很有吸引力。

方案 2 和方案 3 配置可以排除在域控制器上承载 Identity Vault 和 Metadirectory 引擎所存在的性能影响。

在 **Windows** 成员服务器上远程安装

如果对平台有要求，并且存在域控制器的限制，则可以使用三服务器配置。

图 *2-4* 方案 *4* - 三服务器配置



此配置的设置更复杂，但它可以适应某些组织实行的限制。此图中的两台 Windows 服务器是域的成员服务器。

2.3 解决安全问题

要考虑的主要安全问题是鉴定、加密和远程装载程序的使用。如果您具有 Windows 2003 或 Windows 2000 SP3 或更高版本，可以考虑使用一种称为 《签名》的安全选项。请参见 “安全性参数”在第 49 页 中的 《使用签名》。

在管理安全性方面不可能有简单的方案，因为 Windows 提供的安全简报根据 Service Pack、DNS 服务器基础结构、域策略以及服务器上的本地策略设置的不同而不同。以下各节将说明各个安全选项，并提供建议的配置。实施驱动程序和升级组件时，请特别注意安全性。

2.3.1 鉴定方法

通过鉴定，可以让 Active Directory 识别驱动程序 Shim，甚至可以让本地计算机识别驱动程序 Shim。要鉴定到 Active Directory，可以使用 《协商》方法或 《简单》（简单联结）方法。

表 *2-1* 鉴定方法

鉴定方法	说明	优点	缺点
协商	首选方法。 使用 Kerberos*、NTLM 或可插入鉴定模式 （如果安装了其中一种模式的话）。	驱动程序可以在域中的任何服务器上安装。	承载驱动程序的服务器必须是域的成员。

鉴定方法	说明	优点	缺点
简单	如果承载驱动程序 Shim 的服务器不是域的成员，则使用该方法。	驱动程序可以在不是域成员的服务器上安装。	某些供应服务不可用，例如 Exchange 邮箱供应和口令同步。

2.3.2 加密

SSL 可加密数据。根据配置，可以在两个地方使用 SSL：

- Active Directory 驱动程序和域控制器之间
- Identity Vault 和运行 Active Directory 驱动程序的远程装载程序之间

口令同步发生在 Active Directory 和 Identity Vault (eDirectory) 之间。需确保对跨越网络的任何通讯使用 SSL。

如果 Metadirectory 引擎、Identity Vault、Active Directory 驱动程序和 Active Directory 在同一台计算机上，则不需要 SSL。通讯不跨越网络。

但是，如果使用成员服务器上的 Active Directory 驱动程序 Shim 来远程访问 Active Directory，则需要在 Active Directory 驱动程序 Shim 和 Active Directory 之间设置 SSL。要完成此设置，可以在驱动程序配置中将 SSL 参数设置为 《是》。请参见 "远程装载程序和 Identity Manager 之间的 SSL 连接"在第 19 页 中的步骤 5 在第 18 页 。

如果在域控制器上使用远程装载程序，则可以在 Metadirectory 引擎和远程装载程序之间设置 SSL。有关 SSL 和远程装载程序的更多信息，请参见 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）中的 《Setting Up a Connected System》（设置已连接系统）。

下表概括了在 "计划安装"在第 13 页 中介绍的每种方案中，哪些地方可以用到 SSL 连接：

表 **2-2** *SSL* 连接

配置	是否使用 SSL 连接
单服务器	不必要使用 SSL 连接。
两台服务器：Identity Manager 和 Active Directory 驱动程序在同一台服务器上	可以在 Active Directory 驱动程序和域控制器之间建立 SSL 连接。
双服务器：Identity Manager 在一台服务器上，但 Active Directory 驱动程序在另一台服务器上	可以在 Identity Manager 和运行 Active Directory 驱动程序的远程装载程序之间建立 SSL 连接。
三服务器	可以在 Active Directory 驱动程序和域控制器之间建立 SSL 连接。 还可以在 Identity Manager 和运行 Active Directory 驱动程序的远程装载程序之间建立 SSL 连接。

Active Directory 驱动程序和域控制器之间的 **SSL** 连接

要与 Active Directory 域控制器建立 SSL 连接，必须进行设置以使用 SSL。这涉及到设置证书授权者，然后创建、导出和导入必需的证书。

设置证书授权者

大多数组织已有证书授权者。在这种情况下，需要导出有效的证书，然后将它导入到域控制器上的证书储存中。承载驱动程序 Shim 的服务器必须信任该证书的颁发证书授权者所链接到的根证书授权者。

如果组织中没有证书授权者，则必须建立一个证书授权者。Novell、 Microsoft 和某些其它第三方均提供了用于建立证书授权者所必需的工具。建立证书授权者不属于本指南介绍的范围。有关更多信息，请参见

- 《Novell Certificate Server™ 2.5 Administration Guide》（Novell Certificate Server™ 2.5 管理指南）(http://www.novell.com/documentation/lg/crt252/index.html)
- 《Microsoft Step-by-Step Guide to Setting up a Certificate Authority》（Microsoft 设置证书授权者分步指南） (http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp)

创建、导出和导入证书

具备证书授权者以后，要使 LDAP SSL 的操作成功，必须在 LDAP 服务器上安装相应的服务器鉴定证书。同时，承载驱动程序 Shim 的服务器必须信任颁发这些证书的授权者。服务器和客户机都必须支持 128 位加密。

1 生成符合下列 Active Directory LDAP 服务要求的证书：
   - LDAPS 证书位于本地计算机的个人证书储存中 （编程上称为计算机的 《MY 证书储存》）。
   - 与证书匹配的私用密钥位于本地计算机的储存中，并且与证书适当地关联。

     不得为私用密钥启用强私用密钥保护。
   - 《增强型密钥使用》扩展包括服务器鉴定 (1.3.6.1.5.5.7.3.1) 对象标识符 （又称《OID》）。
   - 在下列其中一个位置显示域控制器的 Active Directory 完全限定域名 （例如 DC01.DOMAIN.COM）：
     - 《主题》字段中的常用名 (CN)。
     - 《主题备用名》扩展中的 DNS 项。
   - 证书是由域控制器和 LDAPS 客户机信任的 CA 颁发的。

     要建立信任，可配置客户机和服务器，以信任颁发的 CA 链接到的根 CA。

   此证书允许域控制器上的 LDAP 服务进行侦听，并自动接受 LDAP 和全局编目交通的 SSL 连接。

   注释：Microsoft 知识库文章 321051 《How to Enable LDAP over SSL with a Third-Party Certificate Authority (http://support.microsoft.com/default.aspx?scid=kb;en-us;321051)》中显示了此信息。有关最新要求和更多信息，请查阅本文档。

   ---

2 以 Windows 2000 支持的下列其中一种标准证书文件格式导出此证书：
   - 个人信息交换 （PFX，又称 《PKCS #12》）
   - 加密消息语法标准 (PKCS #7)
   - 判别编码规则 (DER) 二进制 X.509 编码
   - Base64 编码 X.509

3 在域控制器上安装此证书。

下列链接包含每种受支持平台的指导：

- 如何：在 Windows Server 2003 中的万维网服务器上安装导入的证书 (http://support.microsoft.com/default.aspx?scid=kb;en-us;816794)
- 如何：在 Windows 2000 中的万维网服务器上安装导入的证书 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;310178)

请遵循 《将证书导入本地计算机储存》中列出的指导。

4 请确保在承载驱动程序 Shim 的服务器和颁发证书的根证书授权者之间建立信任关系。

承载驱动程序 Shim 的服务器必须信任颁发证书授权者所链接到的根证书授权者。

有关为证书建立信任的更多信息，请参见 《*Windows 2000 Server* 帮助》中的主题 《建立根证书授权者信任的策略》。

5 在 iManager 中编辑驱动程序属性，然后将 《使用 SSL （是 / 否）》选项更改为《是》。

Driver Parameters

SW3K-NDS.VIM

Edit XML

Driver Settings

Polling Interval (min.)	1
Authentication Method	Negotiate
Use Signing (yes/no)	no
Use Sealing (yes/no)	no
Use SSL (yes/no)	yes
Heart Beat	0
Password Sync Timeout (minutes):	5

6 重启动驱动程序。

重启动驱动程序时，将在域控制器和运行 Active Directory 驱动程序 Shim 的服务器之间协商 SSL 连接。

校验证书

要校验证书，请通过 SSL 鉴定到 AD。使用 Windows 服务器上提供的 ldifde 命令行实用程序。要使用 ldifde 命令，请执行下列操作：

1 打开命令行提示符

2 输入 ldifde -f output/input file -t 636 -b administrator domain password -s computerFullName

以下是为端口 636 配置了服务器的情况下，可输入的内容的示例。

ldife -f out.txt -t 636 -b administrator dxad.novell.com novell -s parent1.dxad3.lab.novell

输出将被发送到 out.txt 文件。如果打开文件后看到 Active Directory 中列出了对象，则表示已成功地与 Active Directory 建立了 SSL 连接，并且证书有效。

2.3.3 远程装载程序和 **Identity Manager** 之间的 **SSL** 连接

如果使用的是远程装载程序，则需要在 Metadirectory 引擎和远程装载程序之间设置 SSL，同时在驱动程序和 Active Directory 之间配置设置。

有关在远程装载程序和 Identity Manager 之间建立 SSL 连接的信息，请参见《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的《Setting Up Remote Loaders》（设置远程装载程序）。

2.4 创建管理帐户

在测试环境中，请一直使用管理员帐户，直到 Active Directory 驱动程序开始工作。然后创建一个具有适当权限 （包括受限权限）的管理帐户， Active Directory 驱动程序可专门使用此帐户鉴定到 Active Directory。

如果采取这种做法，更改其它管理帐户时 Identity Manager 管理帐户不受影响。此设计的优势为：

- 可以使用 Active Directory 审计来跟踪 Active Directory 驱动程序的活动。
- 可以像对待其它帐户一样实现口令更改策略，然后对驱动程序配置进行必要的更新。

此帐户的名称和口令储存在驱动程序配置中。因此，只要帐户口令发生更改，就必须更改此口令。如果更改帐户口令但不更新驱动程序配置，则下一次重启动驱动程序时，鉴定将会失败。

要使 《发布者》通道运行，此帐户的域根至少必须有 《读》和 《复制目录更改》权限。对于 《订购者》通道修改的任何对象，还需要有 《写》权限。可以将 《写》权限限制到由《订购者》通道写入的那些树枝和特性。

要衡量 Exchange 邮箱， Identity Manager 帐户必须具有对登录帐户的 " 起操作系统的部分作用 " 许可权限。

要查看删除的对象， Windows 2003 要求具有其它权限。请参见附录 A “更改对 CN=Deleted Objects 树枝的许可权限”在第 81 页 。

2.5 熟悉驱动程序功能

本节介绍在部署 Active Directory 驱动程序之前应该熟悉的驱动程序功能。

2.5.1 多值特性

与版本 2 相比，更改了 Active Directory 驱动程序处理多值特性的方式。

在 " 添加 " 或 " 修改 " 操作中，版本 2 会忽略除第一个更改值以外的所有更改值，从而将 " 订购者 " 通道上的多值特性视为单值特性。Active Directory 驱动程序版本 3 完全支持多值特性。

但是， Active Directory 驱动程序将多值特性与单值特性同步时，会将多值特性视为单值特性。例如，在 Active Directory 中， Telephone Number 特性是单值特性，而在 Identity Vault 中它是多值特性。从 Active Directory 同步该特性时， Identity Vault 中只会储存单值。

这可以在两个特性之间创建真正的同步和映射，但是，如果已映射到单值特性的某个特性含有多个值，则这会导致潜在的数据丢失。在多数情况下，如果您的应用环境需要的话，可以用一个策略将其它值保存在其它位置。

2.5.2 使用自定义布尔特性管理帐户设置

如果在 Microsoft 管理控制台中将帐户设置为在 2006 年 7 月 15 日失效，则 eDirectory 特性 Login Expiration Time 将设置为在 2006 年 7 月 16 日上午 12:00 失效。 Microsoft 管理控制台不允许设置时间值，默认值为 12:00 AM。

驱动程序使用限制性最大的设置。根据您的具体需求，可以在 Microsoft 中对失效时间增加一天。

2.5.3 恢复 Active Directory 对象时保留 eDirectory 对象

在同步通过 Active Directory 工具恢复的任何 Active Directory 对象时，这些对象将删除关联的 eDirectory 对象。Active Directory 驱动程序会查找 Active Directory 对象的 isDeleted 特性发生的更改。如果驱动程序在该特性中检测到更改，则系统将通过驱动程序针对与 Active Directory 对象关联的对象发出删除事件。

如果不希望删除 eDirectory 对象，则必须将其它策略添加到 Active Directory 驱动程序。Identity Manager 3.0 带有一个预定义规则，该规则可以将所有 《删除》事件更改为 《去除关联》事件。有关详细信息，请参见 *《Policy Builder and Driver Customization Guide》*（策略构建器和驱动程序自定义指南）中的 《Command Transformation - Publisher Delete to Disable》（命令转换 - 发布者删除 - 禁用）。

安装 Active Directory 驱动程序 3

3.1 基本步骤

下图说明了在安装 Identity Manager 时可以选择的选项。

图 ***3-1*** *Identity Manager* 安装选项

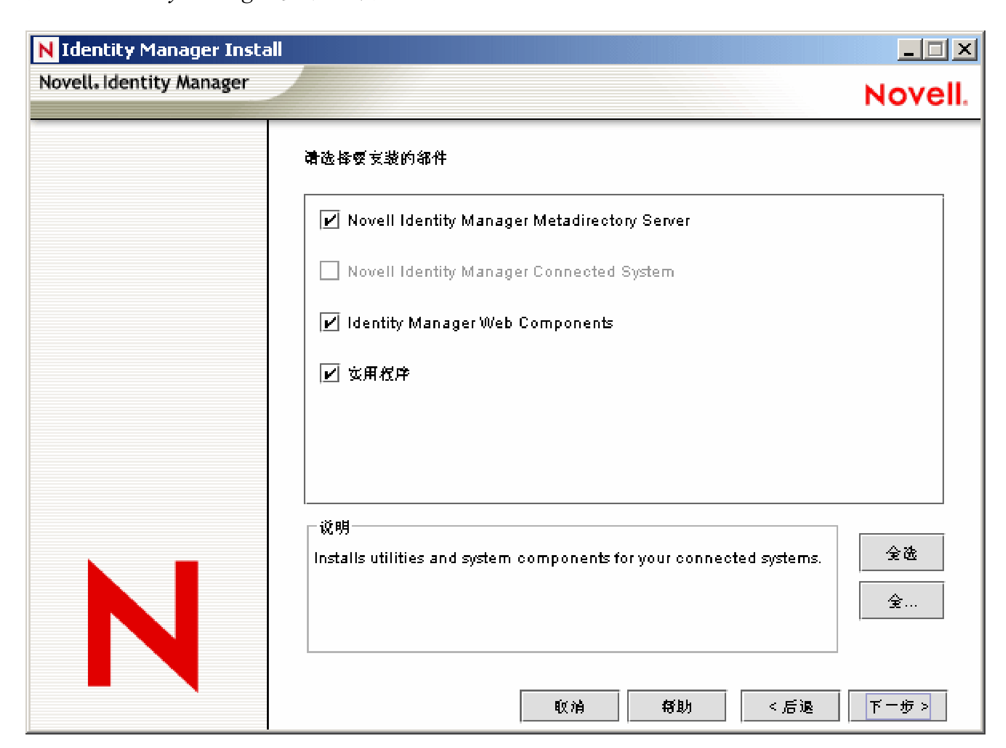


表 ***3-1*** *Identity Manager* 安装选项

选项	说明
Metadirectory 服务器	安装 Metadirectory 引擎和 Identity Manager
已连接系统	安装远程装载程序
Identity Manager 万维网组件	安装预配置 （样本）驱动程序配置文件
实用程序	安装 Active Directory 发现工具

安装 Active Directory 驱动程序 Shim 需要三个基本步骤：

表 **3-2** 安装步骤

步骤	安装期间要选择的选项
1. 在 Metadirectory 引擎服务器或远程装载程序服务器上安装 Active Directory 驱动程序 Shim。	选择 《Metadirectory 服务器》或 《Identity Manager 已连接系统》选项。请参见 “安装 Active Directory 驱动程序 Shim”在第 22 页 。
2. 在 iManager 服务器上安装 Active Directory 的预配置导入文件。	选择 《Identity Manager 万维网组件》选项。请参见 “安装预配置导入文件”在第 27 页 。
3. 在工作站上安装用于配置 Identity Manager 的 Active Directory 发现工具。	选择 《实用程序》选项。请参见 “安装 Active Directory 发现工具”在第 28 页 。

通常，在安装 Metadirectory 服务器 （或远程装载程序）和万维网组件时安装 Active Directory 驱动程序组件。但是，也可以稍后安装这些组件。

3.2 安装 Active Directory 驱动程序 Shim

- “在 Metadirectory 服务器上安装 Shim”在第 22 页
- “在远程装载程序上安装 Shim”在第 25 页

3.2.1 在 Metadirectory 服务器上安装 Shim

1 在运行了 Identity Vault 和 Metadirectory 引擎的服务器上启动 Identity Manager 安装。

从 Identity Manager CD 或下载映象运行安装程序。

2 在 《欢迎》对话框中单击 《下一步》，然后接受许可协议。

3 查看第一个 《Identity Manager 概述》对话框中的信息，然后单击 《下一步》。

该对话框提供有关下列项目的信息：

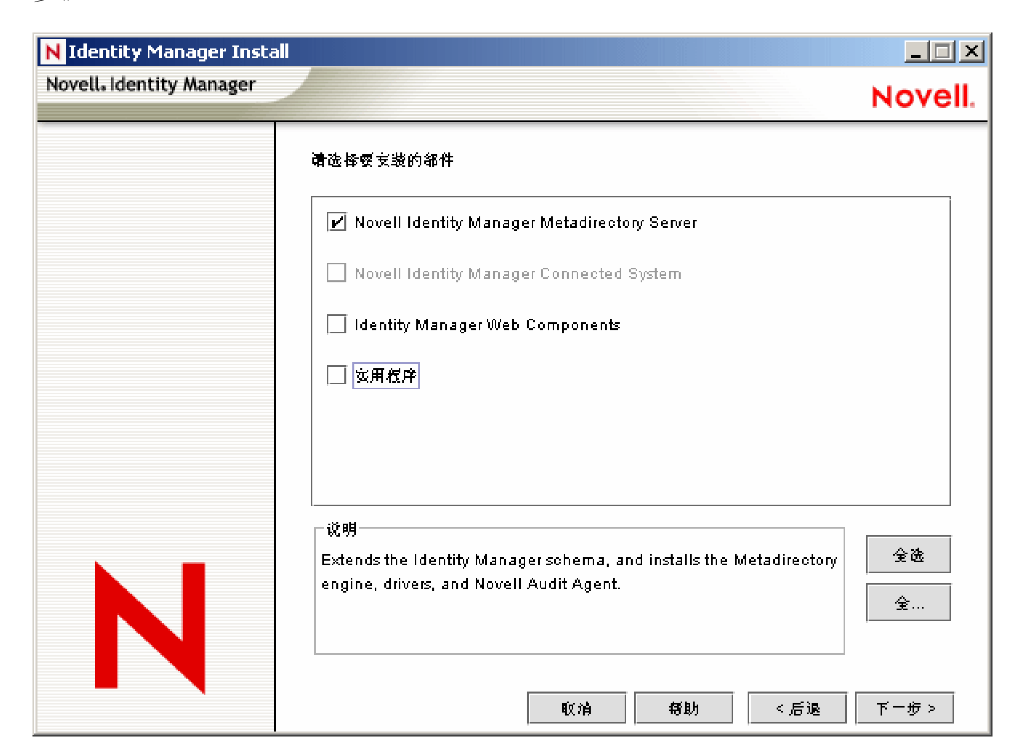
- Metadirectory 服务器
- 已连接系统服务器

4 查看第二个 《Identity Manager 概述》对话框中的信息，然后单击 《下一步》。

该对话框提供有关下列项目的信息：

- 基于万维网的管理服务器
- 实用程序

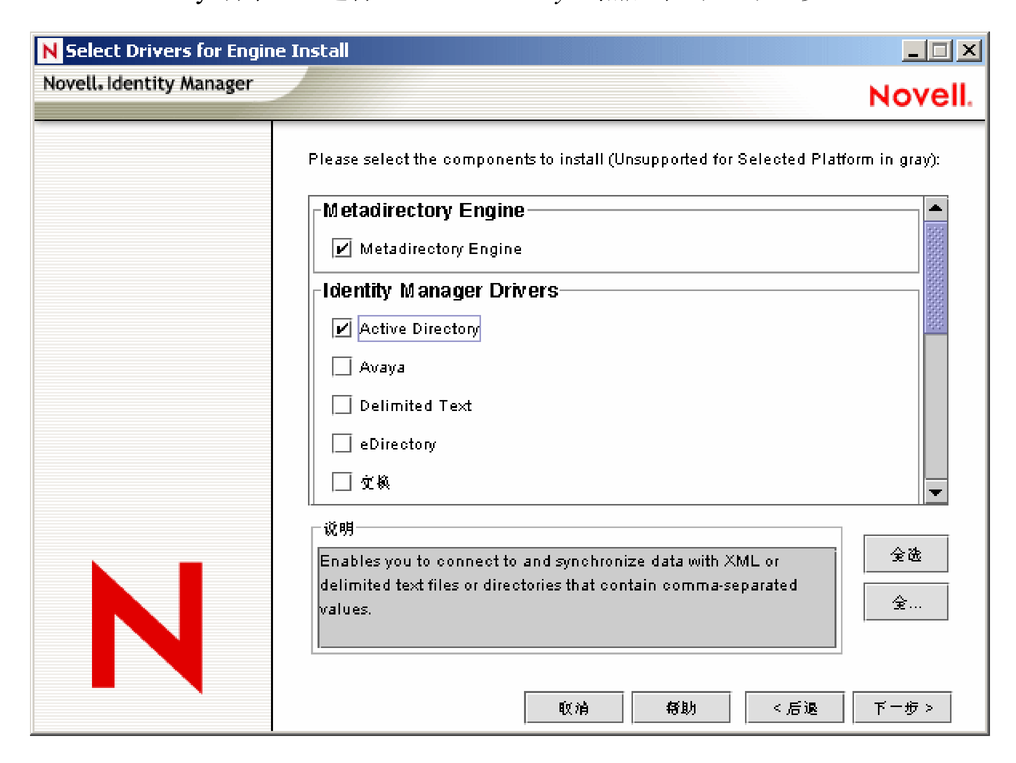
5 在 《请选择要安装的组件》对话框中选择 《Metadirectory 服务器》，然后单击 《下一步》。



如果该计算机上已安装了 iManager，并且此时您想要安装 iManager 插件和配置文件，则还应选择 《Identity Manager 万维网组件》。

如果此时想要安装 Active Directory 管理工具，则还应选择 《实用程序》。

6 在 《Select Drivers for Engine Install （选择用于安装引擎的驱动程序）》对话框中选择《Metadirectory 引擎》，选择 *Active Directory*，然后单击 《下一步》。



7 在 《Identity Manager 升级警告》对话框中单击 《确定》。



8 在 《口令同步升级警告》对话框中单击 《确定》。



9 在 《纲要扩展》对话框中键入用户名和口令，然后单击 《下一步》。

10 查看选择的选项，然后单击 《完成》。

3.2.2 在远程装载程序上安装 Shim

可使用该选项安装 Active Directory 驱动程序 Shim，而该驱动程序 Shim 将在与运行 Metadirectory 引擎的服务器分开的服务器上运行。

1 在运行远程装载程序的服务器上启动 Identity Manager 安装。

   从 Identity Manager CD 或下载映象运行安装程序。

2 在 《欢迎》对话框中单击 《下一步》，然后接受许可协议。

3 查看第一个 《Identity Manager 概述》对话框中的信息，然后单击 《下一步》。

   该对话框提供有关下列项目的信息：

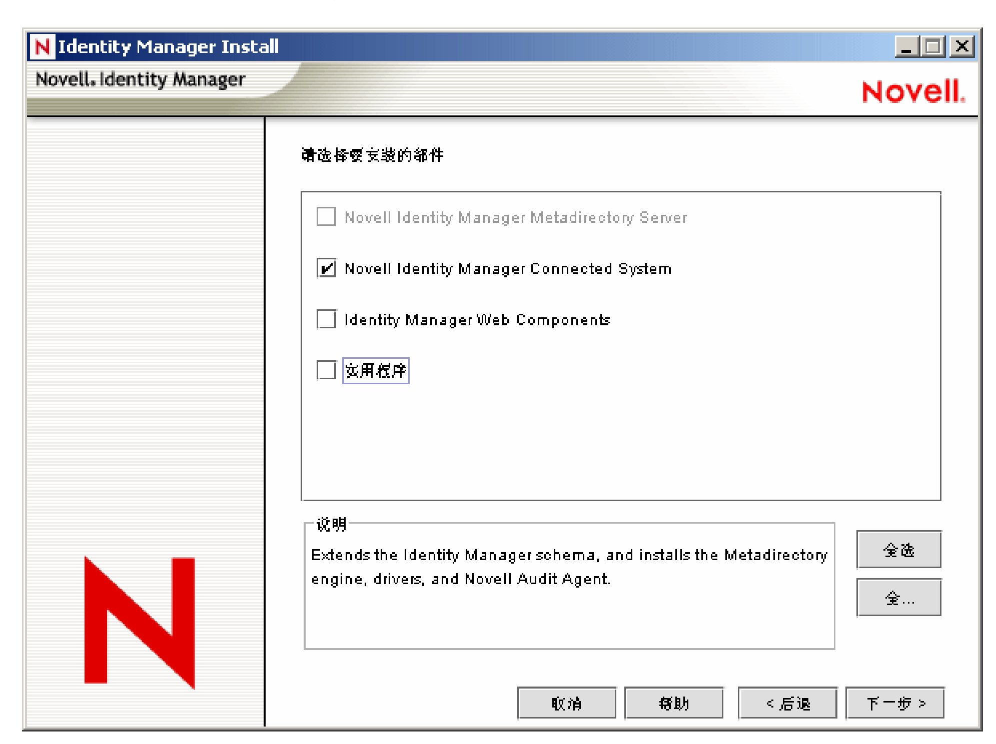
   - Metadirectory 服务器
   - 已连接系统服务器

4 查看第二个 《Identity Manager 概述》对话框中的信息，然后单击 《下一步》。

   该对话框提供有关下列项目的信息：

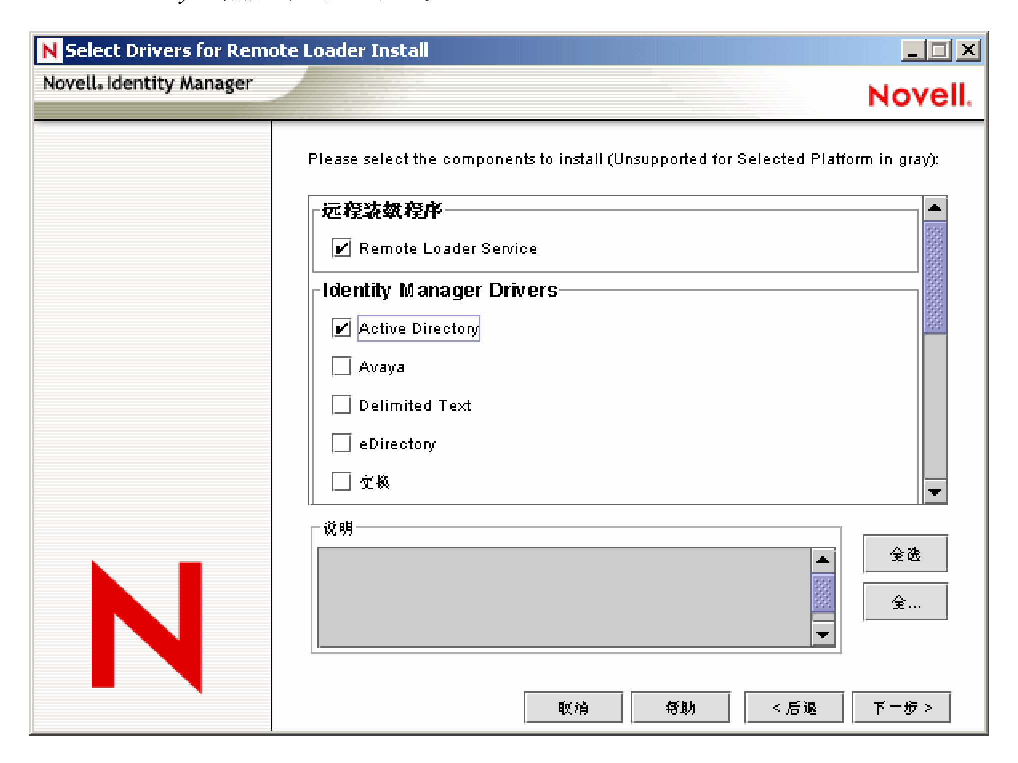
   - 基于万维网的管理服务器
   - 实用程序

5 在 《请选择要安装的组件》对话框中，取消选择 《Metadirectory 服务器》及其它选项，选择 《Identity Manager 已连接系统》，然后单击 《下一步》。



6 指定安装路径，然后单击 《下一步》。

7 在《选择用于安装引擎的驱动程序》对话框中选择《远程装载程序服务》，选择 *Active Directory*，然后单击《下一步》。



8 在《Identity Manager 升级警告》对话框中单击《确定》。



9 在《口令同步升级警告》对话框中单击《确定》。



10 查看选择的选项，然后单击 《完成》。

3.3 安装预配置导入文件

该选项可安装 Identity Manager 的插件，并可安装预配置 （样本）驱动程序配置。安装这些文件后，可以使用 iManager 将 Active Directory 预配置文件导入到驱动程序集，并可以配置驱动程序。

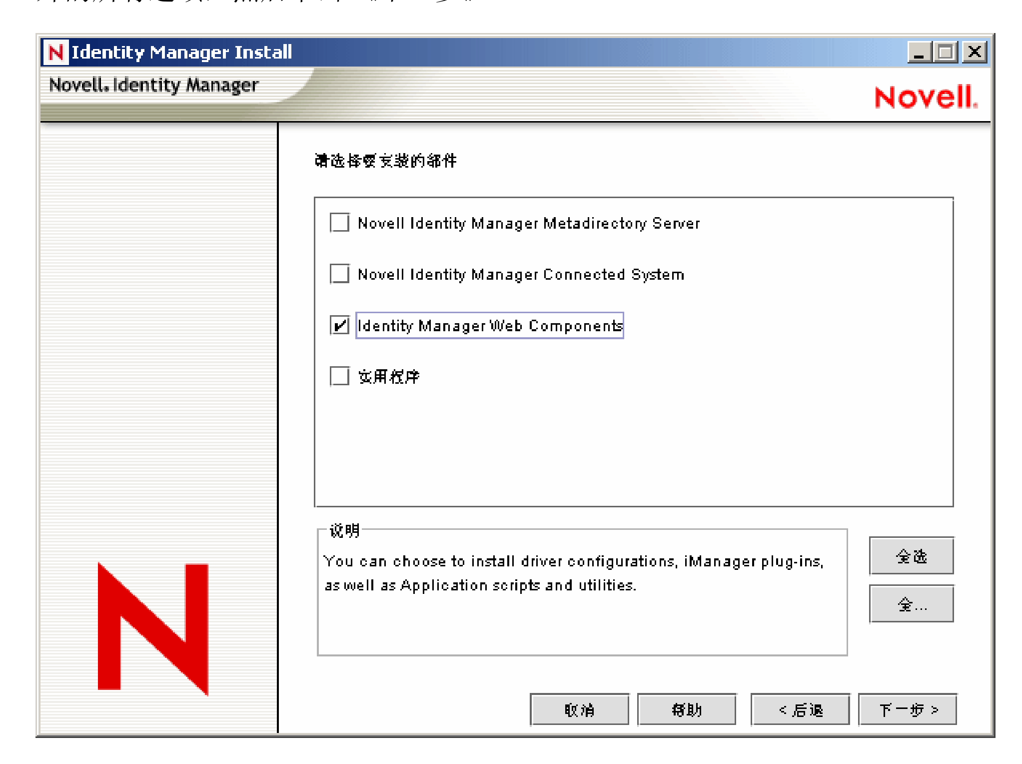
如果安装了 Metadirectory 引擎或远程装载程序，则有可能已安装了这些文件。要单独安装这些文件，请执行下列操作：

1 在安装了 iManager 的服务器上启动 Identity Manager 安装。

2 在 《欢迎》对话框中单击 《下一步》，然后接受许可协议。

3 查看两个 《Identity Manager 概述》对话框中的信息，然后单击 《下一步》。

4 在 《请选择要安装的组件》对话框中，取消选择除 《Identity Manager 万维网组件》以外的所有选项，然后单击 《下一步》。



5 选择 《Identity Manager 驱动程序配置》，然后单击 《下一步》。



可以在安装 Novell iManager 插件时安装驱动程序配置文件，也可以单独安装这些文件。

6 查看选择的选项，然后单击 《完成》。

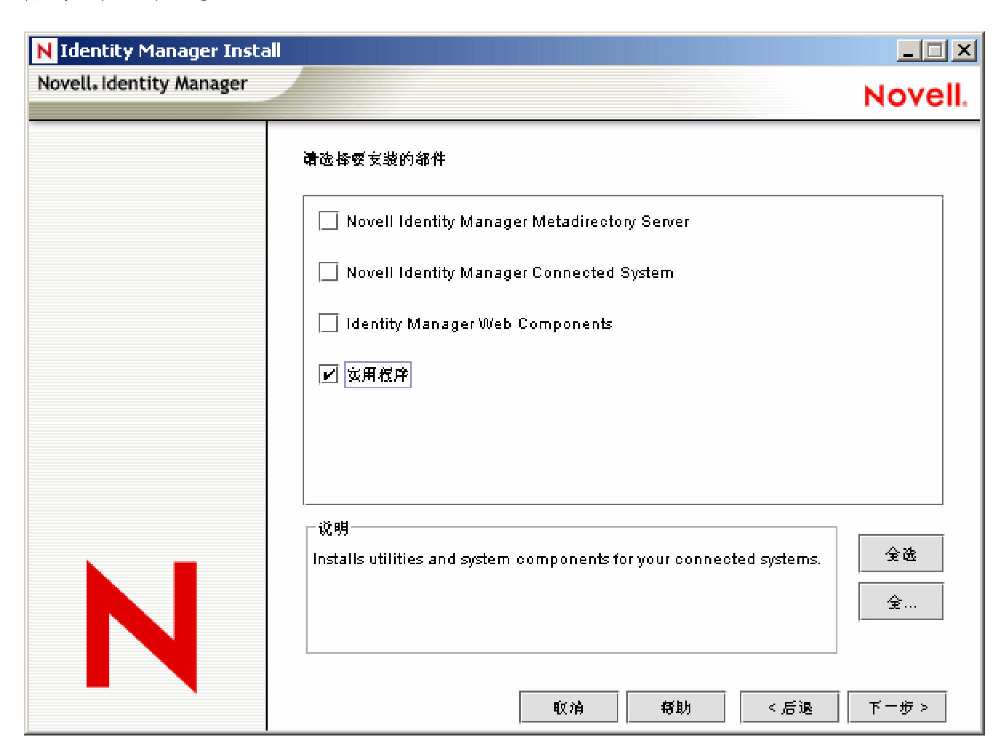
3.4 安装 Active Directory 发现工具

1 在用于配置 Active Directory 的工作站上启动 Identity Manager 安装。

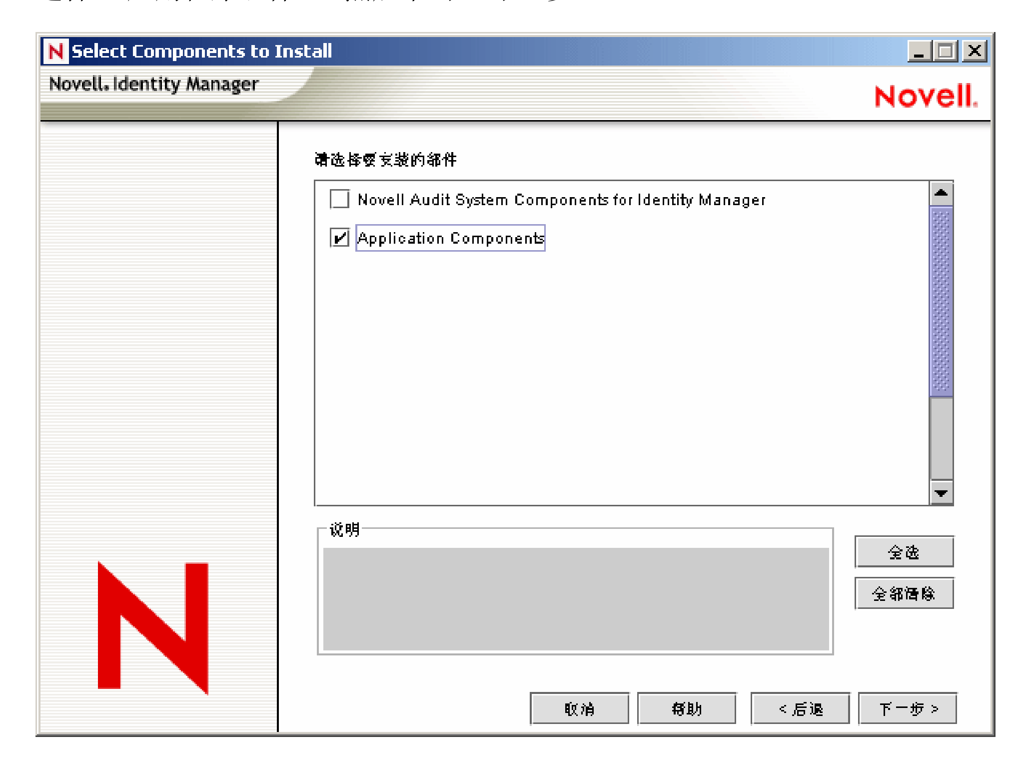
2 在 《欢迎》对话框中单击 《下一步》，然后接受许可协议。

3 查看两个 《Identity Manager 概述》对话框中的信息，然后单击 《下一步》。

4 在《请选择要安装的组件》对话框中，取消选择除《实用程序》以外的所有选项，然后单击《下一步》。



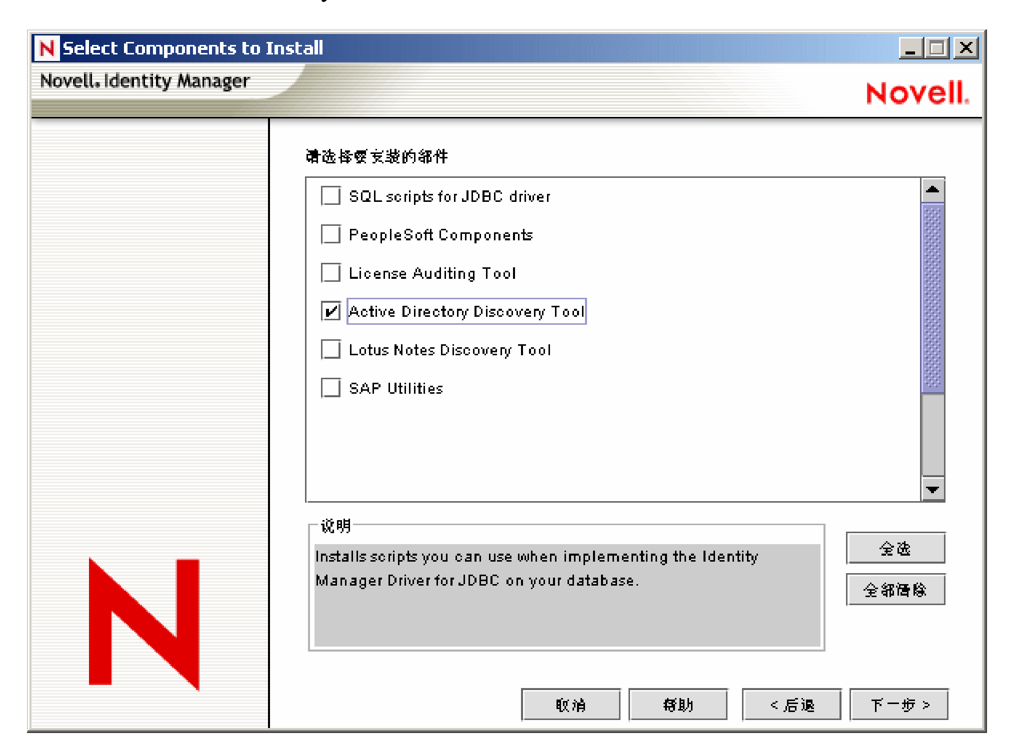
5 选择《应用程序组件》，然后单击《下一步》。



取消选择 Identity Manager 的 Novell 审计系统组件。

6 指定安装路径，然后单击《下一步》。

7 只选择 《Active Directory 发现工具》，然后单击 《下一步》。



8 查看选择的选项，然后单击 《完成》。

配置 Active Directory 驱动程序 4

在 Novell® iManager 中，创建驱动程序向导可帮助导入 Active Directory 基本的驱动程序配置。该向导可以创建和配置使驱动程序正确运行所需的对象。有关使用该向导的详细信息，请参见 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）中的 *《Creating and Configuring a Driver》*（创建和配置驱动程序）。

本节包括：

4.1 在 Designer 中导入驱动程序配置文件

可使用 Designer 导入 Active Directory 基本的驱动程序配置文件。该文件可以创建和配置使驱动程序正确运行所需的对象和策略。以下指导说明如何创建驱动程序，以及如何导入驱动程序的配置。

可以用多种不同的方法导入驱动程序配置文件。本过程只说明其中的一种方法。

1. 在 Designer 中打开一个项目，然后在建模程序中右击驱动程序集对象，再选择 《Add Connected Application （添加已连接应用程序）》。
2. 在下拉列表中选择 *ActiveDirectory.xml*，然后单击 《运行》。
3. 在 《Perform Prompt Validation （执行提示验证）》窗口中单击 《是》。需要填写所有字段才能正确配置 Active Directory 驱动程序。
4. 通过填写字段配置驱动程序。指定特定于环境的信息。有关设置的更多信息，请参见 "配置参数" 在第 32 页 。
5. 指定参数后，单击 《确定》导入驱动程序。
6. 导入驱动程序后，自定义并测试该驱动程序。
7. 完全测试驱动程序后，将驱动程序部署到 Identity Vault。请参见 *《Designer for Identity Manager 3: Administration Guide》*（Designer for Identity Manager 3：管理指南）中的 《Deploying a Driver to an Identity Vault》（将驱动程序部署到 Identity Vault）。

4.2 在 iManager 中导入驱动程序配置文件

Active Directory 预配置文件是一个示例配置文件。在 iManager 服务器上安装了 Identity Manager 万维网组件后，即会安装此文件。请将预配置文件看作导入后针对环境进行自定义或配置的模板。

1. 在 iManager 中选择 《Identity Manager 实用程序》 > 《导入驱动程序》> 。

2 选择一个驱动程序集，然后单击 《下一步》。

要将新驱动程序放在哪个位置?

◉ 在现有驱动程序集中

hraun_set.DigitalAirlines

○ 在新驱动程序集中

如果将此驱动程序放在新的驱动程序集中，则必须指定驱动程序集的名称、环境和关联的服务器。

3 选择 *Active Directory* 驱动程序，然后单击 《下一步》。



4 通过填写配置参数来配置驱动程序。有关设置的信息，请参见 “配置参数”在第 32 页 。

5 使用一个具有某种权限 （驱动程序需要在服务器上具有该权限）的用户对象定义安全性等效

倾向于使用 Admin 用户对象来完成此任务。但是，例如，可能需要创建 DriversUser，然后将安全性等效指派给该用户。无论驱动程序需要在服务器上具有怎样的权限，DriversUser 对象都必须具有相同的安全性权限。

6 标识代表管理职能的所有对象，并将其从复本中排除。

排除在第 2 步指定的安全性等效对象 （例如 DriversUser）。如果删除该安全性等效对象，则会从驱动程序中去除权限。因此，驱动程序不能更改 Identity Manager。

7 单击 《完成》。

4.3 配置参数

下表说明在驱动程序的初始配置期间必须提供的参数。

注释 : 这些参数显示在多个屏幕上。仅当上一个提示的回答需要用于正确配置策略的更多信息时，才会显示其中的某些参数。

表 ***4-1*** 配置参数

字段	说明
驱动程序名	将要指派给该驱动程序的 eDirectory™ 对象名。 由于每个 Active Directory 域都需要一个不同的驱动程序，因此应该将域名包含在驱动程序名中。在查看驱动程序时，就知道该驱动程序与哪个域关联。

字段	说明
鉴定方法	与 Active Directory 进行鉴定的方法。 《协商》为首选方法。选择 《协商》可使用 Microsoft 安全包来协商鉴定。要使用 《协商》，承载驱动程序的服务器必须是域的成员。 如果计划使用口令同步，并且在成员服务器上运行，则需要 SSL。 《简单》使用 LDAP 简单联结。如果选择 《简单》，则建议使用 SSL。 **重要 :** 简单联结不支持口令同步或 Exchange 供应。
鉴定 ID	由 Identity Manager 使用的、具有管理特权的 Active Directory 帐户。使用的名称格式取决于选定的鉴定机制。 对于 《协商》，请提供 Active Directory 鉴定机制所需的名称格式。例如： ◆ 管理员 - AD 登录名 ◆ 域 / 管理员 - 域限定的 AD 登录名 对于 《简单》，请提供 LDAP ID。例如： ◆ cn=DirXML,cn=Users,DC=domain,dc=com
鉴定口令	鉴定 ID 中指定的用户帐户的口令。
鉴定环境	用于同步的 Active Directory 域控制器的名称。 例如，对于 《协商》鉴定方法，可使用 DNS 名称 mycontroller.domain.com。对于 《简单》鉴定方法，可使用服务器的 IP 地址 （例如 10.10.128.23 或 DNS 名称）。 如果不指定任何值，则使用本地主机。 **注释 :** 此值将储存在 Authentication Context 特性中。要在完成初始配置后更改此值，请按照 “安全性参数”在第 49 页 中的说明修改此特性。
域名	此驱动程序管理的 Active Directory 域。 此驱动程序需要采用 LDAP 格式设置的域名：dc=domain,dc=com
域的 DNS 名称	此驱动程序管理的 Active Directory 域的 DNS 名称。 此驱动程序需要采用 DNS 格式设置的域名：domain.com
驱动程序巡回检测间隔	更改发生后， Identity Vault 将更改发送到 Active Directory。但是，只能按照配置的巡回检测间隔来确定将 Active Directory 更改发送到 Identity Vault 的频率。默认值为 1 分钟。 **重要 :** 巡回检测间隔会影响系统性能。巡回检测间隔越小，则搜索越频繁，且数据更新越快。巡回检测间隔偏高会导致交通量的周期性突发。尽管使用偏低巡回检测间隔的总成本较高，但是随着时间的延长，其成本分布更加均匀。 如果将间隔设置为 0 （零），则巡回检测速率为十秒。

字段	说明
口令同步超时 （分钟）	驱动程序尝试同步口令所花费的分钟数。 请将该值设置到大小足以处理所存在的任何口令临时代办事项。如果执行的是大批量更改，请将超时设置到大小足以处理所有的更改。经验法则是每个口令允许一秒钟。例如，要同步 18,000 个口令，则允许 300 分钟 （18,000 个口令除以 60 秒）。 如果设置为 -1，则不限时。尽管此设置可以处理大批量更改，但它会导致出现问题。例如，因为没有对帐户进行关联，所以永远无法对口令进行同步。因此，这样的口令将永远保留在系统中。如果存在许多类似的情况，则会导致系统需要为未同步口令保留较大的库存。 必须至少将口令同步超时设置为巡回检测间隔的三倍。
驱动程序供本地 / 远程使用	选择 《远程》可将驱动程序配置为结合远程装载程序一起使用，选择 《本地》可将驱动程序配置为供本地使用。
远程主机名和端口	仅限 《远程》选项。 安装了远程装载程序服务、且针对此驱动程序运行的主机名或 IP 地址和端口号。默认端口为 8090。 仅当 《驱动程序供本地 / 远程使用》设置为 《远程》时，才显示此设置。
驱动程序口令	仅限 《远程》选项。 远程装载程序使用驱动程序对象口令将其自身鉴定到 Identity Manager 服务器。该口令必须与在远程装载程序上指定为驱动程序对象口令的口令相同。 仅当 《驱动程序供本地 / 远程使用》设置为 《远程》时，才显示此设置。
远程口令	仅限 《远程》选项。 远程装载程序口令用于控制对远程装载程序实例的访问。该口令必须与在远程装载程序上指定为远程装载程序口令的口令相同。 仅当 《驱动程序供本地 / 远程使用》设置为 《远程》时，才显示此设置。
导入将继续进行驱动程序策略选择	仅限 《远程》选项。 如果单击 《确定》，驱动程序向导将使用驱动程序的策略配置继续。
eDirectory 中的基本树枝	在 Identity Vault 中指定需要同步的基本树枝。在订购者匹配策略中使用该树枝来限制同步的 Identity Vault 对象；将对象添加到 Identity Vault 时，发布者布局策略中将使用该树枝。 默认情况下，会将新用户放在该树枝中。使用点分隔格式。例如： users.myorg 如果树枝不存在，则必须在尝试将用户添加到该树枝之前创建该树枝，并确保它与 Active Directory 基本树枝关联。

字段	说明
发布者布局	选择《镜像》可将对象分层次放在基本树枝中。 选择《平面》可将对象严格地放在基本树枝中。 该选择将构建默认的发布者布局策略。 注释：如果选择《镜像》，驱动程序将假定 eDirectory 数据库结构与 eDirectory 基本树枝中的 Active Directory 内的数据库结构相同。如果结构不相同，则不能正确放置对象。在 eDirectory 中的 Active Directory 内创建相同的结构，或者在迁移用户对象之前迁移 eDirectory 树枝。
Active Directory 中的基本树枝	在 Active Directory 中以 LDAP 格式指定基本树枝。默认情况下，会将新用户放在该树枝中。例如： CN=Users,DC=MyDomain,DC=com 如果目标树枝不存在，则必须在尝试将用户添加到该树枝之前创建该树枝，并确保它与 eDirectory 基本树枝关联。 如果创建或使用的树枝不是 Active Directory 中的 Users，则该树枝是 OU 而不是 CN。例如： OU=Sales,OU=South,DC=MyDomain,DC=com
Active Directory 布局	选择《镜像》可将对象分层次放在基本树枝中。 选择《平面》可将对象严格地放在基本树枝中。 该选择将构建默认的订购者布局策略。 注释：如果选择《镜像》，驱动程序将假定 Active Directory 数据库结构与 Active Directory 基本树枝中的 eDirectory 内的数据库结构相同。如果结构不相同，则不能正确放置对象。在 Active Directory 中的 eDirectory 内创建相同的结构，或者在迁移用户对象之前迁移 Active Directory 树枝。

字段	说明
配置数据流	《配置数据流》可以建立能够控制待同步类和特性的初始驱动程序过滤器。此选项的用途在于配置驱动程序，以便以最佳方式表示常规的数据流策略。导入后，可以更改该选项以反映特定的需求。 选择 《双向》可设置类和特性，以便同步 《发布者》和 《订购者》通道。Identity Vault 和 Active Directory 发生的更改会同时在两端进行反映。如果希望两端都成为授权的数据源，请使用此选项。 选择 《AD 到 Vault》可设置类和特性，以便只同步 《发布者》通道。Active Directory 发生的更改将在 Identity Vault 中反映，但 Identity Vault 发生的更改将被忽略。如果希望 Active Directory 成为授权的数据源，请使用此选项。 选择 《Vault 到 AD》可设置类和特性，以便只同步 《订购者》通道。Identity Vault 发生的更改将在 Active Directory 中反映，但 Active Directory 发生的更改将被忽略。如果希望 Vault 成为授权的数据源，请使用此选项。 警告 **:**《删除》、《移动》和 《重命名》事件与过滤器无关。无论选择哪个选项，驱动程序都会处理这些事件。如果不需要同步这些事件，则必须更改驱动程序的默认配置。 可以使用 Identity Manager 3.0 附带的预定义策略之一将 《删除》事件更改为 《去除关联》事件。有关详细信息，请参见 *《Policy Builder and Driver Customization Guide》*（策略构建器和驱动程序自定义）中的 《Command Transformation - Publisher Delete to Disable》（命令转换 - 发布者删除 - 禁用）。 要阻止 《移动》和 《重命名》事件，必须自定义驱动程序。
口令失败通知用户	将配置口令同步策略，以便在口令更新失败时，向关联的用户发送电子邮件通知。可以选择将通知电子邮件的拷贝发送给另一用户（例如安全管理员）。如果需要发送拷贝，请输入或通过浏览找到该用户的 DN。否则，请将该字段留空。
配置权利	可配置驱动程序，以使用权利来管理 Active Directory 中的用户帐户和组成员资格，以及供应 Exchange 邮箱。使用权利时，驱动程序将结合外部服务（例如 Identity Manager 用户应用程序或基于职能的权利）一起工作，以控制供应 （或者在 Active Directory 中取消供应）这些功能时的条件。有关详细信息，请参见 “权利”在第 11 页 。 如果计划使用这些外部服务之一来控制对 Active Directory 的供应，请选择 《是》。 如果不打算使用 Identity Manager 用户应用程序或供应 Exchange 邮箱，请选择 《否》。
用户帐户策略	仅配置 《要素》选项。 Active Directory 中的用户可以由同步控制，也可以使用具有工作流程服务的权利或基于职能的权利进行控制。 选择 《权利》，则将 Active Directory 中的帐户启用控制权限提供给 Identity Vault 中的权利。 选择 《Implement in policy （在策略中实现）》，则使用驱动程序中的策略而不是使用权利。

字段	说明
Exchange 策略	仪配置 《要素》选项。 Exchange 供应可以由驱动程序策略和权利处理，也可以被完全跳过。可以将 Exchange 中的邮箱指派给用户（对用户启用了邮箱），也可以为该用户提供 Identity Vault 记录中储存的外部邮箱有关的信息 （对用户启用了邮件）。如果使用驱动程序策略，是对用户启用邮箱还是启用邮件的决策，以及帐户驻留的 Exchange 讯息数据库，将完全在策略中受到控制。 如果使用 《权利》，则由外部服务 （例如工作流程服务或基于职能的权利）做出这些决策，驱动程序策略只是应用这些决策。 如果选择 《在策略中实现》， 则使用驱动程序中的策略而不是使用权利来指派 Exchange 邮箱。 如果选择 《无》，则默认的配置不创建 Exchange 邮箱，但确实会将 Identity Vault Internet E-Mail Address 与 Active Directory mail 特性同步。
组成员资格策略	仅配置 《要素》选项。 可通过同步成员资格列表或使用权利来控制 Active Directory 中的组成员资格。 选择 《权利》，则使用工作流程服务或基于职能的权利来指派组成员资格。 选择 《同步》，则使用策略来同步组成员资格列表。 选择 《无》，则不同步组成员资格信息。
对 Exchange 使用 CDOEXM （是 / 否）	仅限 《Exchange 策略》选项。 可通过调用 Microsoft Exchange 管理系统控制 Exchange 邮箱，而不是通过常规的特性同步对其进行控制。如果启用此功能，驱动程序 Shim 将截取对 Active Directory homeMDB 特性所做的更改，并调用 CDOEXM （Exchange 管理的协作数据对象）子系统。 在此处选择的值将记录在驱动程序 Shim 配置中。 选择 《是》，则同步 Exchange 邮箱。 选择 《否》，则不同步 Exchange 邮箱。
Allow CDOEXM Exchange mailbox move (yes/no)（允许 CDOEXM Exchange 邮箱移动 （是 / 否））	仅限 《Exchange 策略》选项。 如果启用此功能，驱动程序 Shim 将截取对 Active Directory homeMDB 特性所做的修改，并调用 CDOEXM，以便将邮箱移到新的讯息数据储存中。 选择 《是》，则移动 Exchange 邮箱。 选择 《否》，则不移动 Exchange 邮箱。
Allow CDOEXM Exchange mailbox delete (yes/no)（允许 CDOEXM Exchange 邮箱删除 （是 / 否））	仅限 《Exchange 策略》选项。 如果启用此功能，驱动程序 Shim 将截取对 Active Directory homeMDB 特性的去除操作，并调用 CDOEXM 以删除邮箱。 选择 《是》，则允许删除 Exchange 邮箱。 选择 《否》，则不允许删除 Exchange 邮箱。

字段	说明
Default Exchange MDB（默认的 Exchange MDB）	仅限 《Exchange 策略》 > 《在策略中实现》选项。 输入默认的 Exchange 讯息数据库 (MDB)。例如： [CN=Mailbox Store (CONTROLLER),CN=First Storage Group,CN=InformationStore,CN=CONTROLLER,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=Domain,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=Domain,DC=com] 导入完成后，可以更新驱动程序以管理其它 MDB。
取消帐户权利时	仅限 《Exchange 策略》选项。 用于在权利去除了用户帐户时选择要执行的操作。 *禁用帐户* *删除帐户*
名称映射策略选择 >	驱动程序会将 Identity Vault Full Name 特性映射到 Active Directory 对象名，并将 Active Directory Pre-windows 2000 登录名映射到 Identity Vault 用户名。 可以接受整个策略，也可以手动选择一部分策略。如果策略不符合需求，则可以在导入完成后，通过编辑订购者和发布者命令转换策略中的 NameMap 策略来修改策略。 选择 《接受》，则使用整个策略。 选择 《手动》，则允许您使用策略的一部分。
全名映射	仅限 《名称映射策略选择》 > 《手动》选项。 选择 《是》，则允许驱动程序将 Identity Vault Full Name 特性与 Active Directory 对象名和显示名称保持同步。 选择 《否》，则 Identity Vault Full Name 特性不会与 Active Directory 对象名和显示名称保持同步。 在 Active Directory 中使用 Microsoft 管理控制台的 《用户》和 《计算机》咬接模块创建用户帐户时，此策略将十分有用。
登录名映射	仅限 《名称映射策略选择》 > 《手动》选项。 选择 《是》，则允许驱动程序将 Identity Vault 对象名与 Active Directory Windows 2000 以前版本的登录名 （又称 《NT 登录名》和 《sAMAccountName》）保持同步。 选择 《否》，则不会将 Identity Vault 对象名与 Active Directory Windows 2000 以前版本的登录名保持同步。
导入将继续进行 Windows 2000 登录名策略选择	仅限 《名称映射策略选择》 > 《手动》选项。 *确定*

字段	说明
用户主体名映射	用于选择一种管理 Active Directory Windows 2000 登录名 （又称 《userPrincipalName》）的方法。 userPrincipalName 采用电子邮件地址的格式 （类似于 usere@domain.com）。尽管 Shim 可以将任何值放入 userPrincipalName，但是，除非将域配置为接受与名称一起使用的域名，否则 Shim 作为一个登录名没有作用。 选择 《Follow Active Directory e-mail address （遵循 Active Directory 电子邮件地址）》，则将 userPrincipalName 设置为 Active Directory 邮件特性值。如果希望将用户的电子邮件地址用于鉴定，并且 Active Directory 为电子邮件地址授权，则此选项十分有用。 选择 《Follow Identity Vault e-mail address （遵循 Identity Vault 电子邮件地址）》，则将 userPrincipalName 设置为 Identity Vault 电子邮件地址特性值。如果希望将用户的电子邮件地址用于鉴定，并且 Identity Vault 为电子邮件地址授权，则此选项十分有用。 如果需要根据用户登录名以及策略中定义的硬编码字符串生成 userPrincipalName，则可以使用 《Follow Identity Vault name （遵循 Identity Vault 名称）》。 如果不需要控制 userPrincipalName，或者需要实现自己的策略，则可以使用 《无》。

升级 **Active Directory** 驱动程序 5

5.1 升级核对清单

要升级 Active Directory 驱动程序，请使用以下核对清单。如果您不精通 Identity Manager，则可能需要聘用一个有能力的顾问。

- [ ] 要使用 Password Synchronization 2.0，请添加驱动程序清单和口令策略。

  请参见升级现有的驱动程序配置以支持 Identity Manager 口令同步 (http://www.novell.com/documentation/dirxml20/index.html?page=/documentation/dirxml20/admin/data/bo16oyy.html)。

- [ ] 为持续使用 Password Synchronization 1.0，请将旧策略添加到现有的驱动程序配置。

  请参见将 Password Synchronization 1.0 升级为 Identity Manager 提供的口令同步 (http://www.novell.com/documentation/dirxmldrivers/index.html?page=/documentation/dirxmldrivers/ad/data/bnwjt02.html)。

- [ ] 去除现有驱动程序的样式页中的 sAMAccountName 结构化格式设置。

  sAMAccountName 是 DirXML® 1.1a Active Directory 2.0 驱动程序中的结构化特性。在新的 Active Directory 3.0 驱动程序中，它是一个字符串。

  旧格式：

  ```
     <value type="structured"> <component name="nameSpace">0</
  component> <component association-
  ref="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" name="volume"/> <component
  name="path">jsmith</component> </value>
  ```

  新格式：

  ```
    <add-attr attr-name="sAMAccountName"> <value
  type="string">jsmith</value> </add-attr>
  ```

- [ ] 升级驱动程序配置参数。

  建议在默认情况下使用下列设置：

  ```
  <?xml version="1.0"?> <driver-config name="Active Directory
  Driver"> <driver-options> <pollingInterval display-name="Polling
  Interval (min.)"> 1</pollingInterval> <auth-method display-
  name="Authentication Method"> Negotiate</auth-method> <signing
  display-name="Use Signing (yes/no)" id="> no</signing> <sealing
  display-name="Use Sealing (yes/no)"> no</sealing> <use-ssl display-
  name="Use SSL (yes/no)"> no</use-ssl> <pub-heartbeat-interval
  display-name="Heart Beat"> 0</pub-heartbeat-interval> <pub-
  password-expire-time display-name="Password Sync Timeout
  ```

```
(minutes):">60</pub-password-expire-time> <use-CDOEXM display-
name="Use CDOEXM for Exchange (yes/no)"> no</use-CDOEXM> <cdoexm-
move display-name="Allow CDOEXM Exchange mailbox move (yes/
no)">yes</cdoexm-move> <cdoexm-delete display-name="Allow CDOEXM
Exchange mailbox delete (yes/no)">yes</cdoexm-delete> </driver-
options> </driver-config>
```

- ❑ 将鉴定 ID 转换为 Sam 帐户名 （例如 jsmith）或 《域名 / 帐户名》格式 （例如域 / jsmith）。
- ❑ 将 Login Disabled 特性映射由 userAccountControl 更改为 dirxml-uACAccountDisable。
- ❑ 如果供应的是 Exchange 帐户，请将 CDOEXM 的驱动程序参数更改为 《是》，然后从现有的驱动程序配置样式页中去除下列四个硬编码特性：
  - msExchHomeServerName
  - legacyExchangeDN
  - homeMTA
  - msExchMailboxSecurityDescriptor
- ❑ 如果从 Identity Manager 2.x 升级，并且启用了 Exchange 供应，则必须将一个覆盖应用到驱动程序。Identity Manager 3.0 可控制对 Exchange 邮箱的移动和删除。要使这种功能对升级的驱动程序起作用，必须应用覆盖。有关如何应用覆盖的信息，请参见 "应用 Exchange 邮箱的覆盖" 在第 43 页 。

5.2 Login Disabled 值寻址

eDirectory™ 将缺少条件 Login Disabled = true 视为 Login Disabled = false。因此，如果以新安装 （不是升级）的形式安装 Active Directory 版本 3，并且值 Login Disabled = false 不存在，创建规则上的默认策略将合成该值。

默认情况下，从版本 2 驱动程序升级为版本 3 驱动程序不能获取该策略。

5.3 从 DirXML 1.1a 升级驱动程序 Shim

升级会将以前的驱动程序 Shim 替换为新的驱动程序 Shim，但是会保留以前的驱动程序的配置。新的驱动程序 Shim 可以运行 DirXML 1.1a 配置且不对其进行更改 （除非运行了 Password Synchronization 1.0）。

如果继续使用 Password Synchronization 1.0，则不需要升级驱动程序 Shim。DirXML 1.1a 驱动程序 Shim 可以在 Identity Manager 3.0 引擎上运行，但是 Identity Manager 3.0 驱动程序 Shim 不能在 DirXML 1.1a 引擎上运行。

如果不选择升级驱动程序 Shim，请确保在安装 Identity Manager 3.0 引擎期间取消选择 Active Directory 驱动程序。如果选择它，则会升级驱动程序 Shim。

要升级驱动程序 Shim，请执行下列操作：

1. 确保已使用当前运行版本的所有增补程序更新了驱动程序。

   建议对所有驱动程序执行此步骤，以帮助将升级问题减至最低程度。

2. 安装 Identity Manager 3.0 驱动程序 Shim。可以在安装 Identity Manager 3.0 引擎的同时执行此步骤。

遵循 *《Identity Manager 3.0 安装指南》*的 《安装 Identity Manager》一节中的指导。

警告 : 如果使用的是 Password Synchronization 1.0，则只能在已阅读 “将 Password Synchronization 1.0 升级为 Identity Manager 提供的口令同步” 在第 57 页 ，并且已准备好将策略添加到驱动程序配置，以便与 Password Synchronization 1.0 向后兼容的情况下，才可以安装升级的 Identity Manager Driver for AD。

不支持将 Identity Manager 2.0 或 3.0 驱动程序 Shim 或配置与 DirXML 1.1a 引擎一起运行。

3 安装 Shim 之后，需要重启动 Novell eDirectory 和驱动程序。

3a 在 iManager 中单击 《Identity Manager》 > 《Identity Manager 概述》。

3b 通过浏览找到驱动程序所在的驱动程序集，然后单击 《搜索》。

3c 单击驱动程序图标的右上角，然后单击 《重启动驱动程序》。

4 使用 Identity Manager 激活身份凭证激活驱动程序 Shim。

请参见 “激活驱动程序” 在第 53 页 。

安装驱动程序 Shim 之后，继续第 4 章 “配置 Active Directory 驱动程序” 在第 31 页 。

5.4 从 IDM 2.*x* 升级驱动程序 Shim

1 确保已使用当前运行版本的所有增补程序更新了驱动程序。

建议对所有驱动程序执行此步骤，以帮助将升级问题减至最低程度。

2 安装 Identity Manager 3.0 驱动程序 Shim。可以在安装 Identity Manager 3.0 引擎的同时执行此步骤。

遵循 *《Identity Manager 3.0 安装指南》*的 《安装 Identity Manager》一节中的指导。

警告 : 如果使用的是 Password Synchronization 1.0，则只能在已阅读 “将 Password Synchronization 1.0 升级为 Identity Manager 提供的口令同步” 在第 57 页 ，并且已准备好将策略添加到驱动程序配置，以便与 Password Synchronization 1.0 向后兼容的情况下，才可以安装升级的 Identity Manager Driver for AD。

不支持将 Identity Manager 驱动程序 Shim 或配置与 DirXML 1.1a 引擎一起运行。

3 安装 Shim 之后，需要重启动 Novell eDirectory 和驱动程序。遵循 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）的《Starting, Stopping, or Restarting a Driver》（启动、停止或重启动驱动程序）中的指导。

4 使用 Identity Manager 激活身份凭证激活驱动程序 Shim。

请参见 “激活驱动程序” 在第 53 页 。

安装驱动程序 Shim 之后，继续第 4 章 “配置 Active Directory 驱动程序” 在第 31 页 。

5.5 应用 Exchange 邮箱的覆盖

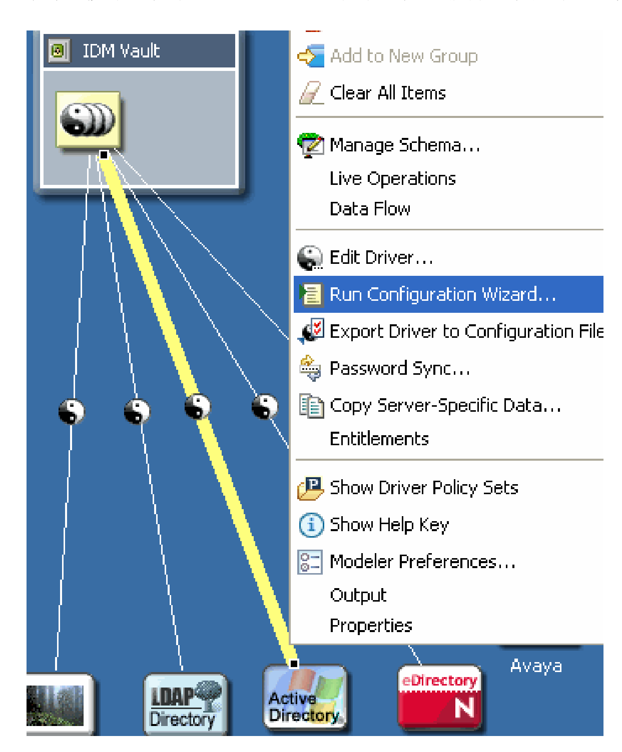
如果已将 Identity Manager 2.x 升级为 Identity Manager 3.0，并且在驱动程序上启用了 Exchange 供应，则需要应用 AD 驱动程序覆盖。驱动程序可使用覆盖来控制对 Exchange 邮箱的删除和移动。

- “在 Designer 中应用覆盖” 在第 44 页

- “在 iManager 中应用覆盖”在第 47 页

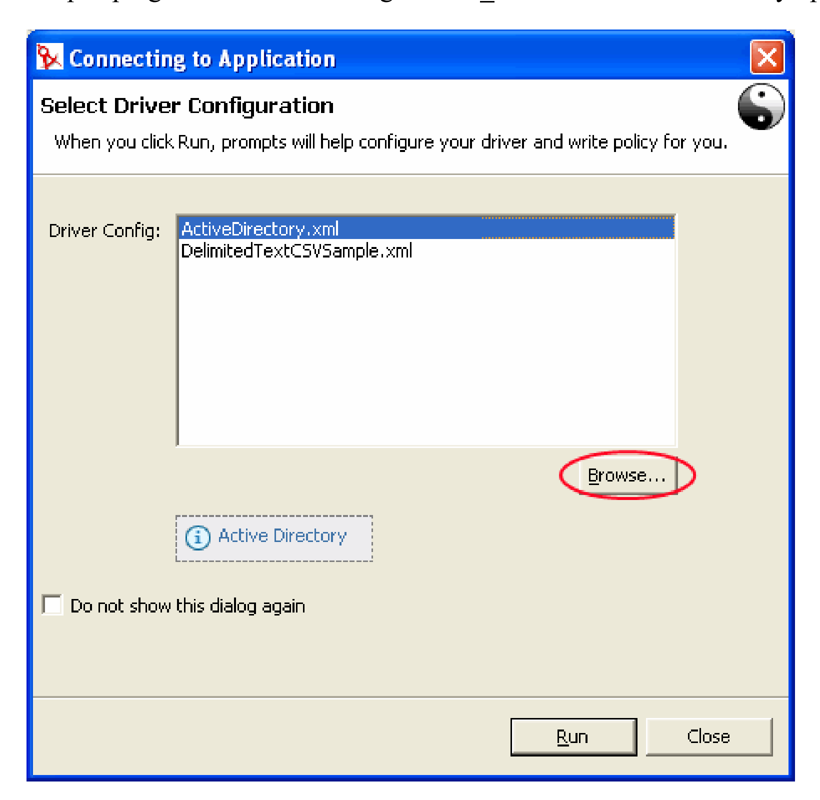
5.5.1 在 Designer 中应用覆盖

1 在建模程序中右击 AD 驱动程序连接程序图标，然后单击 《运行配置向导》。



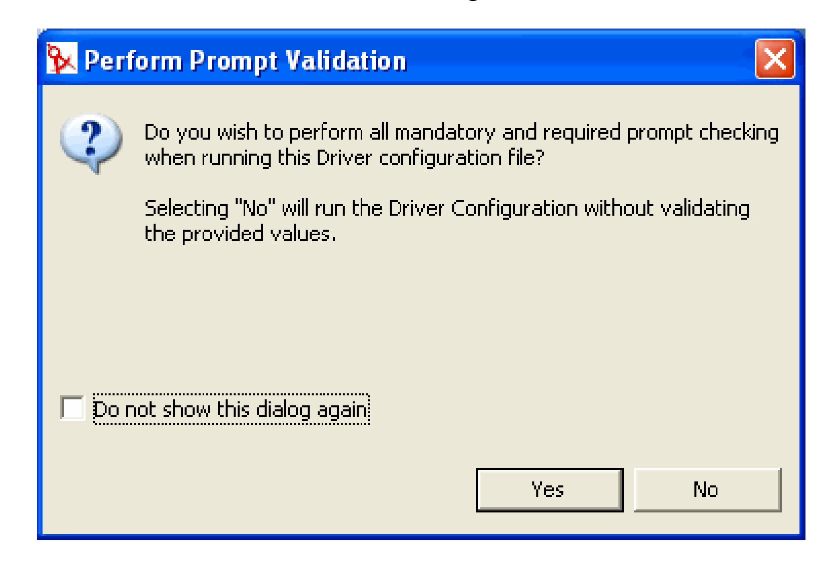
2 选择 《浏览》并找到文件 ActiveDirectoryUpdate.xml，然后单击 《打开》> 。

该文件位于以下插件中：
eclipse\plugins\com.novell.designer.idm_*x.x.x*\defs\ActiveDirectoryUpdate.xml。



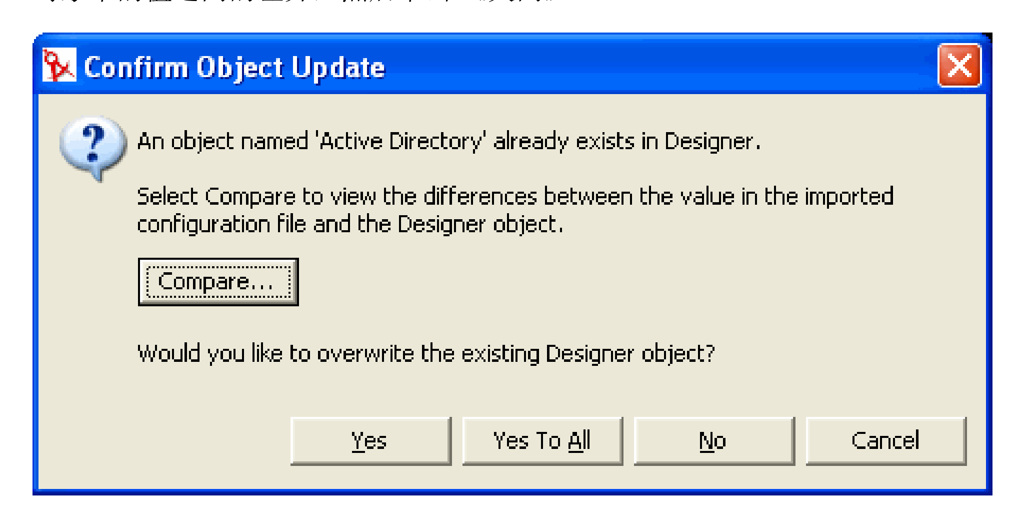
3 选择 *ActiveDirectoryUpdate.xml*，然后单击 《运行》。

4 选择 《是》；或者，如果需要 Designer 验证在提示中输入的信息，请选择 《否》> 。



5 请输入特定于环境的信息，然后单击《确定》。有关字段的说明，请参见表 5-1 在第 46 页。

6 在 《确认对象更新》窗口中选择 《比较》，以查看已导入配置文件中的值和 Designer 对象中的值之间的差异，然后单击 《关闭》。



7 如果更改正确，请选择 《是》重写现有的 Designer 对象。如果不需要更新驱动程序，请选择 《否》。

表 ***5-1*** *Designer* 中的覆盖配置参数

参数	说明
驱动程序名	这是需要使用新参数更新的驱动程序。输入驱动程序名，或浏览并选择驱动程序。
更新驱动程序	可使用参数更新驱动程序。如果需要更新驱动程序，请选择 《是》。如果不需要更新驱动程序，请选择 《否》。
homeMDB 控制 Exchange 移动	如果允许更改用户 HomeMDB 特性，则用户使用 CDOEXM 时，其 Exchange 邮箱会移动。用户的邮箱将要移到的 Exchange 讯息数据库必须与原有的 Exchange 讯息数据库在同一个域中。 如果选择 《是》，那么将用户对象移到 eDirectory 中后，Active Directory 和 Exchange 中也会反映移动。 如果选择 《否》，那么将用户对象移到 eDirectory 中后，Active Directory 中会反映该对象，但 Exchange 中不反映。
homeMDB 控制 Exchange 删除	允许去除用户 HomeMDB 特性，以便当用户使用 CDOEXM 时，删除其 Exchange 邮箱。 如果选择 《是》，那么删除某个 eDirectory 用户对象后，将会删除关联的 Active Directory 用户对象和 Exchange 帐户。 如果选择 《否》，那么删除某个 eDirectory 用户对象后，将会删除关联的 Active Directory 用户对象，但 Exchange 帐户保持不变。

参数	说明
登录和模拟	允许 CDOEXM 的驱动程序鉴定帐户和口令集支持以不同方式登录。 如果选择 《否》，则驱动程序只执行网络登录。 如果选择 《是》，则驱动程序执行本地登录。鉴定帐户必须是具有管理特权的 Active Directory 帐户。

5.5.2 在 iManager 中应用覆盖

可以使用两种方法通过 iManager 更新驱动程序。可以在 Identity Manager 概述中更新驱动程序，也可以通过 Identity Manager 实用程序更新。

Identity Manager 概述

1. 在 iManager 中选择 《Identity Manager》 > 《Identity Manager 概述》。
2. 选择 《搜索》可查找储存 Active Directory 驱动程序的驱动程序集对象。
3. 在 《Identity Manager 概述》屏幕中选择 《添加驱动程序》。
4. 浏览并选择储存 Active Directory 驱动程序的驱动程序集对象，然后单击 《下一步》。
5. 选择 《从服务器中导入驱动程序配置 （.XML 文件）》。
6. 在下拉菜单中选择 《ActiveDirectoryUpdate.xml》，然后单击 《下一步》。
7. 输入特定于环境的信息，然后单击《下一步》。有关字段的说明，请参见表 5-2 在第 47 页。
8. 选择 《Update that driver (including the driver 謂 image) （更新该驱动程序 （包括驱动程序的映象））》以更新该驱动程序，或者选择 《选择另一个驱动程序》，然后单击 《下一步》。
9. 查看更改摘要，然后单击 《完成》。

表 **5-2** *iManager* 中的覆盖配置参数

参数	说明
驱动程序名	这是需要使用新参数更新的驱动程序。
现有的驱动程序	从下拉菜单中选择启用了 Exchange 供应的已更新 AD 驱动程序的名称。选择驱动程序名后，系统会自动填充 《驱动程序名》字段。
更新驱动程序	可使用参数更新驱动程序。如果需要更新驱动程序，请选择 《是》。如果不需要更新驱动程序，请选择 《否》。
homeMDB 控制 Exchange 移动	如果允许更改用户 HomeMDB 特性，则用户使用 CDOEXM 时，其 Exchange 邮箱会移动。用户的邮箱将要移到的 Exchange 讯息数据库必须与原有的 Exchange 讯息数据库在同一个域中。 如果选择 《是》，那么将用户对象移到 eDirectory 中后， Active Directory 和 Exchange 中也会反映移动。 如果选择 《否》，那么将用户对象移到 eDirectory 中后， Active Directory 中会反映该对象，但 Exchange 中不反映。

参数	说明
homeMDB 控制 Exchange 删除	允许去除用户 HomeMDB 特性，以便当用户使用 CDOEXM 时，删除其 Exchange 邮箱。 如果选择 《是》，那么删除某个 eDirectory 用户对象后，将会删除关联的 Active Directory 用户对象和 Exchange 帐户。 如果选择 《否》，那么删除某个 eDirectory 用户对象后，将会删除关联的 Active Directory 用户对象，但 Exchange 帐户保持不变。
登录和模拟	允许 CDOEXM 的驱动程序鉴定帐户和口令集支持以不同方式登录。 如果选择 《否》，则驱动程序只执行网络登录。 如果选择 《是》，则驱动程序执行本地登录。鉴定帐户必须是具有管理特权的 Active Directory 帐户。

Identity Manager 实用程序

1. 在 iManager 中选择 《Identity Manager 实用程序》 > 《导入驱动程序》。
2. 浏览并选择储存 Active Directory 驱动程序的驱动程序集对象，然后单击 《下一步》。
3. 在 《Additional Policies （其它策略）》中选择 《AD Driver shim configuration update from IDM2 to IDM 3 （将 AD 驱动程序 Shim 配置由 IDM 2 更新为 IDM 3）》，然后单击《下一步》。

   ☐ 

   从 IDM2 到 IDM 3 的 AD 驱动程序 Shim 配置更新

4. 输入特定于环境的信息，然后单击《下一步》。有关字段的说明，请参见表 5-2 在第 47 页。
5. 选择 《更新该驱动程序 （包括驱动程序的映象）》以更新该驱动程序，或者选择 《选择另一个驱动程序》，然后单击 《下一步》。
6. 查看更改摘要，然后单击 《完成》。

管理 Active Directory 驱动程序 6

6.1 安全性参数

在安装过程中，驱动程序将会收集必需的信息，并创建默认的安全性策略和参数。开始自定义 Active Directory 驱动程序之前，应该熟悉以下项目：

- 默认的策略和参数
- 第 8 章 "查错"在第 75 页中介绍了这些主题，以便您可以确定这些问题是否适用于您的环境

了解这些参数的相互配合方式以及与操作系统的配合方式，有助于确定实现 Identity Manager 数据同步安全性的方法。

- 鉴定 **ID**：驱动程序用来访问域数据的帐户。

表 ***6-1*** 鉴定 *ID*

格式	用户名	方法
域名	用户	协商
完全限定的域名	域 \ 用户	协商
判别名	cn=DirXML,cn=Users,DC=domain,dc=com	简单

- 鉴定环境：用于访问域数据的环境。

表 ***6-2*** 鉴定环境

格式	示例	方法
活动域控制器的 DNS 名称	mycontroller.mydomain.com	协商
活动域控制器的 DNS 名称，或 LDAP 服务器的 IP 地址	mycontroller.mydomain.com 137.65.134.83	简单

- 应用程序口令： 鉴定 ID 帐户的口令。
- 使用签名：此参数可以在 Active Directory 驱动程序和 Active Directory 之间使用，但不能在 Metadirectory 引擎和远程装载程序之间使用。签名可确保恶意计算机不会截取数据。如果没有使用 LDAP SSL 端口，则此标志可启用 Active Directory 连接的签名。

此设置需要在两台服务器上使用 Windows 2003 或带有最新支持包的 Windows 2000，以及 Internet Explorer 5.5 SP2 或更高版本。这可以启用 Kerberos 或 NTLM v2 已鉴定连接的签名。

与 SSL 一样，此参数对初始导入不可用。安装完成后可通过 《驱动程序参数》页设置该参数。

- 使用签署：此参数可以在 Active Directory 驱动程序和 Active Directory 之间使用，但不能在 Metadirectory 引擎和远程装载程序之间使用。签署可以加密数据，使网络监视程序不能查看这些数据。如果没有使用 LDAP SSL 端口，则此标志可启用 Active Directory 连接的签署。

  此设置需要在两台服务器上使用 Windows 2003 或带有最新支持包的 Windows 2000，以及 Internet Explorer 5.5 SP2 或更高版本。这可以启用对 Kerberos 或 NTLM v2 已鉴定连接的加密。

  与 SSL 一样，此参数对初始导入不可用。安装完成后可通过 《驱动程序参数》页设置该参数。

- 使用 **SSL**：此参数可以在 Active Directory 驱动程序和 Active Directory 之间使用。如果使用 LDAP SSL 端口连接到 Active Directory，则此参数可控制加密。此参数适用于《协商》和 《简单》鉴定方法。

  默认情况下，此参数设置为 《否》。如果将此值设置为 《是》，则为整个对话加密 SSL 管道。由于驱动程序通常会同步敏感信息，因此最好使用加密的管道。但是，加密将会减慢服务器的常规性能。

  导入驱动程序之后，可通过 《驱动程序参数》页配置此参数。

6.1.1 建议的安全性配置

使用 **Identity Manager** 远程装载程序

表 ***6-3*** 建议的设置

参数	**说明**
鉴定 ID	域登录名，例如 Administrator。
鉴定环境	域控制器的 DNS 名称。
	如果不需要在 Active Directory 域控制器上运行驱动程序，请对 《协商》方法使用*主机名*，但是对 《简单》方法使用*主机名*或 IP 地址。
应用程序口令	鉴定帐户使用的口令。
远程装载程序口令	远程装载程序服务的口令。
鉴定方法	协商。
使用签名	否。需要在两台服务器上使用 Windows 2003 或带有最新支持包的 Windows 2000，以及 Internet Explorer 5.5 SP2 或更高版本。
使用签署	否。需要在两台服务器上使用 Windows 2003 或带有最新支持包的 Windows 2000，以及 Internet Explorer 5.5 SP2 或更高版本。
使用 SSL	是。如果驱动程序 Shim 没有在域控制器上运行，则执行订购者口令检查、设置和修改时需要 SSL。

使用 **SSL**

如果选择了《简单》鉴定机制，则建议使用 SSL，因为《简单》鉴定以明文形式传递口令。

表 ***6-4*** *SSL* 参数

参数	说明
鉴定 ID	LDAP 格式鉴定 ID
鉴定环境	域控制器的 IP 地址
口令	指定的鉴定 ID 的口令
使用签名	否
使用签署	否
使用 SSL	是

6.2 管理组

Active Directory 组类为组中的成员资格定义了两个组类型和三个作用域。类型和作用域由 groupType 特性控制，在 Active Directory 中创建一个组以及通过修改特性更改该组后，可通过 Identity Manager 策略设置 groupType 特性。

组可以保存对象参照的集合。分发组类型不向其成员指定任何特殊的权限或特权，并通常用作 Exchange 的分发列表。安全组类型是安全主体。其成员可接收组的权限和特权。安全组具有一个 pre-Windows 2000 登录名 (samAccountName) 和一个安全标识符 (SID)，可以在其它对象的安全描述符 (SD) 访问控制列表 (ACL) 中使用该 SID。

组作用域控制异域中的对象是否可以是组的成员，以及组本身是否可以是另一个组的成员。三个作用域是《本地域》、《全局》和《通用》。这些作用域的工作方式，或者作用域是否完全有效，取决于 Active Directory 是否以 Windows 2000 混合方式、Windows 2000 纯方式或 Windows 2003 方式运行。

一般而言，《本地域》组可以保存对林中任何位置的对象的参照，但只能在域中为这些组指派许可权限。《全局》组与此相反。它们只能保存对域中对象的参照，但是可以通过林为这些组指派许可权限。《通用》组可以保存参照，并且可以通过林为这些组指派许可权限。但是《通用》组自身存在一些限制和性能问题。应该在遵照 Microsoft 建议的条件下创建和使用这些组。

groupType 特性是一个 32 位整数，它的位可定义类型和作用域。在任何给定的时间，组只能有一个作用域。

表 ***6-5*** *GroupType* 特性

GroupType 特性	作用域	定义类型和作用域的位
GROUP_TYPE_GLOBAL_GROUP	分发	0x00000002
GROUP_TYPE_DOMAIN_LOCAL_GROUP	分发	0x00000004

GroupType 特性	作用域	定义类型和作用域的位
GROUP_TYPE_UNIVERSAL_GROUP	分发	0x00000008
GROUP_TYPE_SECURITY_ENABLED	安全性	0x80000000

6.3 管理 Microsoft Exchange 邮箱

可以配置 Active Directory 驱动程序，使之能够创建、移动和删除 Active Directory 中的用户的 Microsoft Exchange 邮箱。可通过设置和去除用户对象的 homeMDB 特性值来管理邮箱。该特性保存邮箱驻留的 Exchange 私用讯息数据库 (MDB) 的判别名。驱动程序只能管理与它在同一域中的 Exchange 服务器上的邮箱。

可通过多种不同的方法管理 Exchange 邮箱。默认的配置通过订购者命令转换策略中做出的策略决策来管理邮箱。如果用户符合给定的条件，则会创建、移动或去除邮箱。导入文件为邮箱管理提供三个选项：

- 权利
- 策略
- 不管理 Exchange 邮箱

如果使用权利方法进行供应，则根据在 Identity Vault 中针对某个用户设置的权利为该用户授予或拒绝邮箱。权利保存 MDB 的判别名以及一个状态值，该值告知驱动程序是否授予或取消了权利。权利自身由用户应用程序或基于职能的权利驱动程序管理。无论哪种情况，外部工具都将授予（或取消）对邮箱的权限，订购者命令转换策略会将该权限转换为 homeMDB 特性上的添加值或去除值，驱动程序 Shim 会将 homeMDB 的更改转换为对 Exchange 管理系统的适当调用。

如果使用权利，并且组织中有多个 MDB，则可以使用用户应用程序来确定将哪个 MDB 指派给给定的用户。 《Identity Manager Accessory Portlet Reference Guide》(http://www.novell.com/documentation/idm) （Identity Manager 附属入口小程序参考指南）包含有关如何配置多个 MDB 的文档。Identity Manager 驱动程序的职能是响应用户对象上放置的权利，而不是将这些权利放置在用户对象上。如果使用用户应用程序，那么当工作流程项目流经批准过程时，将为您提供一个用于选择的 Exchange MDB 列表。如果使用基于职能的权利，则会将 MDB 指派给保存用户职能的组。

如果使用基于策略的方法进行供应，订购者命令转换策略将使用 Identity Vault 中的用户对象的状态相关信息来对 MDB 进行指派。驱动程序 Shim 会将更改转换为对 Exchange 管理系统的适当调用。默认的策略使用简单规则指派邮箱。该策略假定只有一个 MDB，并且假定到目前为止通过策略链生成该 MDB 的所有用户均应被指派给该 MDB。由于用于指派不同 MDB 的规则随公司的不同而有很大的差异，因此默认的配置不会尝试建立 《正确的方法》来执行指派。只需更改默认的指派规则便可以实现自己的策略。使用 DirXML 底稿 if 语句来定义邮箱指派的条件，并使用 homeMDB 特性的 do-set-dest-attribute 命令来影响更改。可以使用 ADManager.exe 工具或使用自己的方法来获取 Exchange MDB 列表。

不管理 Exchange 邮箱时，驱动程序会将用户的电子邮件地址与邮件绰号进行同步。

还可以通过其它方法管理 Exchange 邮箱。例如，可以扩展 Identity Vault 的纲要以保存 homeMDB 信息，并使用基本数据同步将邮箱指派给 Active Directory 中的用户。在这种情况下，可以使用自己的工具在 Identity Vault 中进行指派。

对单个 MDB 进行简单的邮箱指派时，默认策略可发挥良好的作用。如果需要策略反映环境中要求的更复杂的规则，则必须更改策略。

6.4 激活驱动程序

在安装后的 90 天内激活驱动程序。90 天试用期过期后，如果没有适当的激活身份凭证，则不能启动驱动程序。无法激活时发生的事件，将在激活时以及以后启动驱动程序时进行处理。

有关激活的信息，请参考 《*Identity Manager 3.0 安装指南*》中的 《激活 Novell Identity Manager 产品》。

口令同步 7

本节的内容假定您熟悉 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Password Synchronization across Connected Systems》（在已连接系统间同步口令）。本节中的信息特定于该驱动程序。

重要：如果以前使用了 Password Synchronization 1.0，则应该在阅读了 "将 Password Synchronization 1.0 升级为 Identity Manager 提供的口令同步"在第 57 页 并理解其中的含义后，才安装新的驱动程序 Shim。如果安装驱动程序 Shim，则需要同时将 Password Synchronization 1.0 的向后兼容性添加到驱动程序策略，即使不打算立即使用 Identity Manager 提供的口令同步，也是如此。

本节包括：

有关口令同步查错的信息，请参见 "口令同步的提示"在第 77 页 。

7.1 比较 Password Synchronization 1.0 与 Identity Manager 提供的口令同步

表 *7-1* 不同版本的口令同步之间的差异

功能	在 Password Synchronization 1.0 中	在 Identity Manager 提供的口令同步中
产品交付	与 Identity Manager 分开交付的产品。	Identity Manager 包含的一项功能，不作为单独的产品出售。

功能	在 **Password Synchronization 1.0** 中	在 **Identity Manager** 提供的口令同步中
平台	◆ Active Directory ◆ NT 域	以下平台支持完全的双向口令同步： ◆ Active Directory ◆ eDirectory™ ◆ NIS ◆ NT 域 这些已连接系统支持将用户口令发布到 Identity Manager。由于通用口令和分发口令可互逆，因此 Identity Manager 可将口令分发到已连接系统。 支持订购者口令要素的任何已连接系统可以从 Identity Manager 中订购口令。 请参见 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）中的《Password Synchronization across Connected Systems》（在已连接系统间同步口令）。
eDirectory 中使用的口令	eDirectory 口令 （不可逆）	通用口令 （可逆）或分发口令 （亦可逆）。如果需要，还可以将 eDirectory 口令保持同步。有关示例方案，请参见 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）中的《Implementing Password Synchronization》（实现口令同步）。
Windows 已连接系统的主要功能	提供双向口令同步，以便 eDirectory 口令与 Windows 口令同步。但是，每个工作站都需要 Novell® Client™。	提供双向口令同步。由于通用口令与分发口令可逆，因此可以朝两种方向同步口令。在 Identity Manager 《发布者》和 《订购者》通道中完成。
LDAP 口令更改	不受支持。	受支持。
Novell Client	必需。	不需要。
nadLoginName 特性	用于保持口令的已更新状态。	不使用。
包含口令同步功能的组件	Identity Manager 驱动程序包含用于更新 nadLoginName 的功能。	驱动程序配置中的策略提供口令同步功能。驱动程序只是执行 Metadirectory 引擎给定的任务，这些任务来自策略中的逻辑。 驱动程序清单、全局配置值和驱动程序过滤器设置也必须支持口令同步。这些设置包含在样本驱动程序配置中，也可以将这些设置添加到现有的驱动程序。请参见 “升级现有的驱动程序配置以支持 Identity Manager 口令同步”在第 62 页 。
代理	一套独立的软件。	未安装代理，而该功能现在是驱动程序的一部分。

7.2 将 Password Synchronization 1.0 升级为 Identity Manager 提供的口令同步

如果当前使用的是 Password Synchronization 1.0，请遵循本节中的指导完成升级。

重要 : 请在查看这些指导之后才安装 Identity Manager 驱动程序 Shim。

要将 Password Synchronization 1.0 升级为 Identity Manager 提供的口令同步，请执行下列操作：

1 确保环境已准备好使用通用口令。

请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Preparing to Use Identity Manager Password Synchronization and Universal Password》（准备使用 Identity Manager 口令同步和通用口令）。

启用通用口令不会自动地使两个系统中的口令发生更改。仅当用户更改了他们的口令后，通用口令同步才开始运行。

方案：通用口令。在 DigitalAirlines，网络管理员 Sandy 启用了通用口令。用户 Markus 登录并更改了其口令。两个系统均为 Markus 设置了通用口令。但是，用户 Marie 登录后未更改其口令。她使用未更改的口令继续登录。Marie 更改其口令之前，系统不会为其设置通用口令功能。

2 安装 Identity Manager 3 驱动程序 Shim 以替换 DirXML® 1.1a 驱动程序 Shim，然后立即完成步骤 3。

注释 : 如果运行的是 Identity Manager 2.0，并且使用了通用口令，则不必要升级口令同步。

使用 《*Identity Manager 3.0 安装指南*》的 《安装 Identity Manager》一章中说明的安装程序，并且只选择 Identity Manager Driver for Active Directory。

3 按 “通过添加策略创建 Password Synchronization 1.0 的向后兼容性”在第 59 页 中的说明将新策略添加到驱动程序配置，创建 Password Synchronization 1.0 的向后兼容性。

DirXML 1.1a 驱动程序 Shim 可更新 nadLoginName 特性，但是 Identity Manager 驱动程序 Shim 不更新该特性。因此，必须将策略添加到驱动程序配置，以更新 nadLoginName。这样，在安装驱动程序 Shim 时， Password Synchronization 1.0 可照常工作。因此，在完成部署 Identity Manager 口令同步时，不会丢失口令更改。

重要 : 如果不创建向后兼容性， Password Synchronization 1.0 将继续更新现有的用户，但是，在部署 Identity Manager 口令同步之前，不能同步任何新用户或重命名的用户。

完成此步骤之后，将会拥有 Identity Manager 3.0 驱动程序 Shim 以及用于实现向后兼容的策略。因此，驱动程序可支持 Password Synchronization 1.0。

如果不能立即完成此过程余下的部分，则可以继续使用 Password Synchronization 1.0，直到准备好完成部署 Identity Manager 口令同步。

4 将 Identity Manager 口令同步的支持添加到希望其参与口令同步的每个驱动程序。

升级或替换现有的配置。

升级现有的配置： 可通过将现有的 DirXML 1.1a 驱动程序配置转换为 Identity Manager 格式，并添加 Identity Manager 口令同步所需的策略，来升级该驱动程序配置：

- 使用向导将驱动程序转换为 Identity Manager 格式。请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的《Upgrading Existing Driver Configurations to Support Password Synchronization》（升级现有的驱动程序配置以支持口令同步）。
- 添加策略以支持 Identity Manager 口令同步。可以使用 《覆盖》配置文件一次性添加策略、驱动程序清单和 GCV。还必须将特性添加到过滤器。有关指导，请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Upgrading Existing Driver Configurations to Support Password Synchronization》（升级现有的驱动程序配置以支持口令同步）。

将现有配置替换为 **Identity Manager** 配置，然后再次添加向后兼容性。 Identity Manager 样本驱动程序配置包含支持 Identity Manager 口令同步所需的策略、驱动程序清单、 GCV 和过滤器设置。有关导入新驱动程序配置的信息，请参见本驱动程序指南的第 4 章 "配置 Active Directory 驱动程序" 在第 31 页 中的指导。

- 如果选择替换现有的配置，请确保按 "通过添加策略创建 Password Synchronization 1.0 的向后兼容性" 在第 59 页 中的说明再次添加向后兼容性。Identity Manager 样本驱动程序配置不包含这些策略。
- 确保将 nadLoginName 特性设置为 《发布》，因为该特性曾经包含在以前的驱动程序配置中。

5 如果需要已连接系统向 Identity Manager 提供用户口令，请安装新的口令同步过滤器，并对其进行配置。

请参见 "设置口令同步过滤器" 在第 65 页 。

6 必要时设置 SSL。

有关指导，请参见 "解决安全问题" 在第 15 页 。

驱动程序在 Active Directory （《订购者》通道）中设置口令的功能需要下列其中一个条件提供安全的连接：

- 运行驱动程序的计算机与域控制器是同一台计算机。
- 运行驱动程序的计算机与域控制器在同一个域中。
- 对于不在域中的计算机，需要在该计算机与域控制器之间设置 《简单》方法和 SSL。仅当使用 《协商》鉴定机制时，双向口令同步才可用。

  有关指导，请参考 Microsoft 文档，例如 《在域控制器上配置数字证书 (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp)》。

7 通过创建启用了通用口令的口令策略，为 Identity Vault 用户帐户打开通用口令。

请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Managing Password Synchronization》（管理口令同步）。

为简化管理，建议尽量在树的最上层指派口令策略。

8 使用驱动程序的口令策略和口令同步设置，设置需要用于口令同步的方案。

请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Implementing Password Synchronization》（实现口令同步）。

9 测试口令同步。

10 Identity Manager 口令同步运行后，去除 Password Synchronization 1.0。

10a 使用添加 / 去除程序，通过去除代理来关闭 Password Synchronization 1.0。

10b 在驱动程序的过滤器中，将 nadLoginName 特性更改为 《忽略》。

10c 去除从驱动程序配置更新 nadLoginName 的向后兼容性策略。

10d 如果需要，在 Identity Manager 口令同步运行后，还可以从用户中去除 nadLoginName 特性，因为不再需要该特性。

7.2.1 通过添加策略创建 Password Synchronization 1.0 的向后兼容性

Password Synchronization 1.0 依赖于可更新名称为 nadLoginName 的特性的驱动程序 Shim。该特性指示是否应同步用户的口令。如果添加了新用户，或者用户的名称发生更改，则系统会添加或更新 nadLoginName 特性以进行匹配。

因为 Identity Manager 口令同步不需要该特性，所以 Identity Manager 中的驱动程序 Shim 不再更新该特性。因此，安装新的驱动程序 Shim 之后，nadLoginName 特性将不进行更新。这意味着，除非将向后兼容性添加到驱动程序配置，否则 Password Synchronization 1.0 不再接收有关新用户或已命名用户的通知。

要从 Password Synchronization 1.0 平稳地转换到 Identity Manager 口令同步，需要与 Password Synchronization 1.0 向后兼容。

要做到与 Password Synchronization 1.0 向后兼容，必须添加更新 nadLoginName 特性的策略。

无论是更新现有的驱动程序配置，还是将这些配置替换为 Identity Manager 附带的新配置，都必须添加这些策略。默认情况下， Active Directory 的 Identity Manager 样本驱动程序配置不包括策略。

必需三个策略，分别用于订购者输出转换、发布者输入转换和发布者命令转换。Identity Manager 的一个名称为 Password Synchronization 1.0 Policies for Active Directory 的配置文件中提供了这些策略。以下过程说明如何导入新策略并将其添加到驱动程序配置。

1 在 iManager 中单击 《Identity Manager 实用程序》 > 《导入驱动程序》 。

将打开导入驱动程序向导。

2 选择现有 Active Directory 驱动程序所驻留的驱动程序集，然后单击 《下一步》。

3 在显示的驱动程序配置列表中，滚动到 《其它策略》区域，选择 《Legacy Password Synchronization 1.0 Policies: （旧的 Password Synchronization 1.0 策略：）Backwards Compatibility for AD and NT （AD 和 NT 的向后兼容性）》，然后单击 《下一步》。

4 完成导入提示：

4a 选择现有的 Active Directory 驱动程序。

可通过选择现有的驱动程序添加三个必需的策略。导入过程将创建三个新的策略对象，其后，您必须将这些对象插入到驱动程序配置中的相应位置。

4b 指定驱动程序是否为 Active Directory 驱动程序。

根据选择的系统，导入的策略存在微小的差异。

4c 浏览并选择与需要更新的驱动程序相关联的 nadDomain 对象。

该对象通常在驱动程序对象下面。

4d （仅限 Active Directory）指定要映射到 Active Directory 特性 sAMAccountName 的 eDirectory™ 特性的名称。

可以在驱动程序配置的纲要映射策略中找到此信息。

注释：如果不将 sAMAccountName 映射到任何 eDirectory 特性，请将 sAMAccountName 映射到 DirXML-ADAlias name。

---

5 单击 《下一步》。

由于选择了一个现有的驱动程序，因此将显示一个页，要求您确定如何更新驱动程序。在这种情况下，只需更新选定的策略。

6 选择 《只更新该驱动程序中的选定策略》，然后选中所有三个列出的策略的复选框。

7 单击 《下一步》，然后单击 《完成》以完成向导。

至此，驱动程序对象下方已创建三个用作策略对象的新策略，但是这些策略还不是驱动程序配置的一部分。要链接这些策略，必须在 《订购者》和 《发布者》通道上，将每一个策略手动插入到驱动程序配置中的正确位置。

8 将三个新策略中的每一个插入到现有驱动程序配置中的正确位置。

如果驱动程序配置的这些部分中的任一部分具有多个策略，请确保最后列出这些新策略。

表 *7-2* 策略

策略对象名	策略的插入位置
PassSync(Pub) 命令转换策略	《发布者》通道上的命令转换策略
PassSync(Pub) 输入转换策略	《发布者》通道上的输入转换策略
PassSync(Sub) 输出转换策略	《订购者》通道上的输出转换策略

针对每个策略重复步骤 8a 至 8f。

8a 单击 《Identity Manager》 > 《Identity Manager 概述》> 。

8b 选择所更新的驱动程序的驱动程序集。

8c 单击刚刚更新的驱动程序。

将打开一个页，其中显示驱动程序配置的图形表示形式。

8d 单击需要将三个新策略之一添加到的位置的图标。

8e 单击 《插入》以添加新策略。

在显示的 《插入》页中单击 《使用现有策略》，通过浏览找到新策略对象，然后单击 《确定》。

8f 在列表中，如果三个新策略中的任何一个具有多个策略，请使用箭头按钮 向下移动新策略，使之位于列表的最后位置。

9 针对所有的 Active Directory 驱动程序重复步骤 1 至 9。

如果需要将 sAMAccountName 映射到 《发布者》通道纲要映射策略中的 DirXML-ADAliasName，则请遵循该过程。

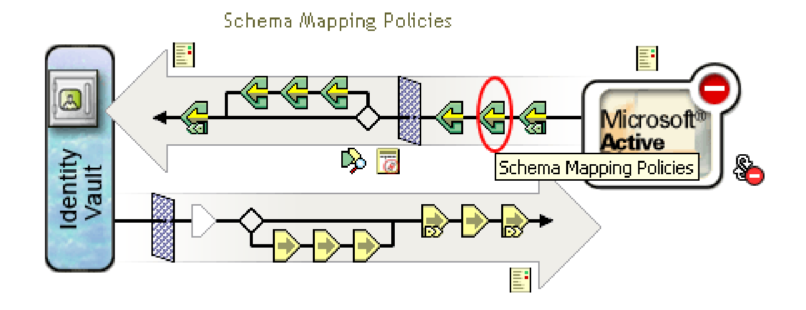
警告：如果 sAMAccountName 已映射到另一个特性，则遵循该过程会使策略失效。策略将停止同步口令。确保在步骤 4d 在第 59 页 中输入正确的特性。

---

1 在 iManager 中选择 《Identity Manager》 > 《Identity Manager 概述》。

2 浏览并选择包含 Active Directory 驱动程序的驱动程序集对象，然后单击 《搜索》。

3 单击驱动程序图标，然后单击 《发布者》通道的 《纲要映射策略》图标。



4 单击 《编辑》。

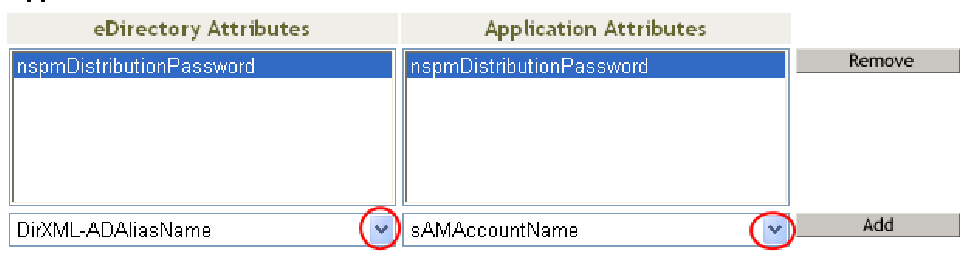
5 选择 《用户》类，然后单击 《特性》。

Driver DN: ADExchange.Driver Set.Novell

eDirectory Classes	Application Classes	
User	user	Remove
Group	group	Attributes...
Organizational Unit	organizationalUnit	
Organization	organization	
Locality	locality	
[Anything]	<No Unmapped Classes>	Add

6 单击 《eDirectory 特性》下面的下拉列表，然后浏览并选择 《DirXML-ADAliasName》。

7 单击 《应用程序特性》下面的下拉列表，然后浏览并选择 《sAMAccountName》。



8 单击 《添加》，然后单击 《确定》。

9 选择 《组》类，然后单击 《特性》。

10 针对 《组》类重复步骤 6 至 8。

11 单击 《确定》两次。

完成此过程后， Active Directory 驱动程序的驱动程序配置将与 Password Synchronization 1.0 向后兼容。这意味着口令同步将像往常一样继续工作，使您可以在方便的时候升级到 Identity Manager 口令同步。

7.3 新的驱动程序配置和 Identity Manager 口令同步

如果使用的不是 Password Synchronization 1.0，并且准备创建新的驱动程序，或者将现有驱动程序的配置替换为 Identity Manager 配置，那么，请遵循 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）的 《Configuring and Synchronizing a New Driver》（配置和同步新驱动程序）中的指导。

此外，请执行下列操作：

- 必要时设置 SSL。请参见 "解决安全问题" 在第 15 页 。

  驱动程序在 Active Directory （《订购者》通道）中设置口令的功能需要下列其中一个条件提供安全的连接：

  - 运行驱动程序的计算机与域控制器是同一台计算机。
  - 运行驱动程序的计算机与域控制器在同一个域中。
  - 对于不在域中的计算机，需要在该计算机与域控制器之间设置 《简单》方法和 SSL。仅当使用协商鉴定机制时，双向口令同步才可用。

    有关指导，请参考 Microsoft 文档，例如 《启用 SharePoint Portal Server 2003 的安全套接层 (http://office.microsoft.com/en-us/assistance/HA011648191033.aspx)》。

- 如果需要已连接系统向 Identity Manager 提供用户口令，请安装新的口令同步过滤器，并对其进行配置。请参见 "设置口令同步过滤器" 在第 65 页 。
- 使用驱动程序的口令策略和口令同步设置，设置需要使用的口令同步方案。请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Implementing Password Synchronization》（实现口令同步）。

7.4 升级现有的驱动程序配置以支持 Identity Manager 口令同步

重要：如果驱动程序与 Password Synchronization 1.0 一起使用，则应该将本节作为 "将 Password Synchronization 1.0 升级为 Identity Manager 提供的口令同步" 在第 57 页 的一部分来完成，而不应独立完成。

下面概述必须使用本节的过程来完成的任务：

- 将驱动程序清单、全局配置值和口令同步策略添加到驱动程序配置。有关要添加的策略的列表，请参见 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）中的 《Policies Required in the Driver Configuration》（驱动程序配置中所需的策略）。
- 更改过滤器，以允许对 nspmDistributionPassword 特性启用订购者通知和发布者忽略功能。

前提条件

- ❑ 确保按 《*Novell Identity Manager 3.0 Administration Guide*》（Novell Identity Manager 3.0 管理指南）的 《Upgrading a Driver Configuration from DirXML 1.1a to Identity Manager Format》（将驱动程序配置由 DirXML 1.1a 升级为 Identity Manager 格式）中的说明，将现有的驱动程序转换为 Identity Manager 格式。
- ❑ 使用导出驱动程序向导为现有的驱动程序创建备份。

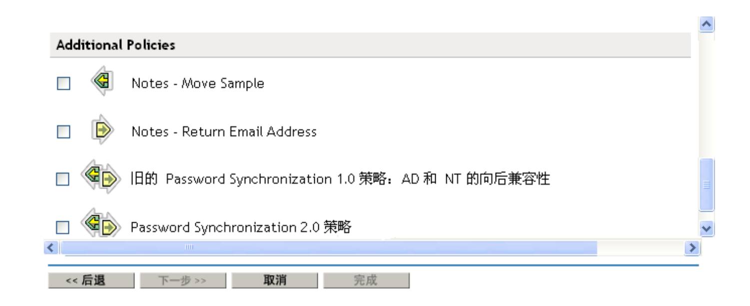
❑ 确保安装新的驱动程序 Shim。如果没有 Identity Manager 驱动程序 Shim，某些口令同步功能 （例如 《检查口令状态》）将无法工作。

过程

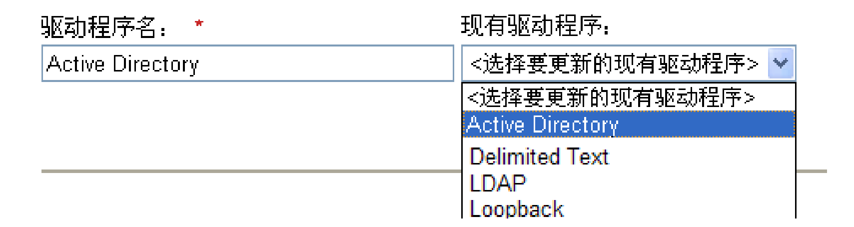
1 在 iManager 中单击 《Identity Manager 实用程序》 > 《导入驱动程序》。

将打开导入驱动程序向导。

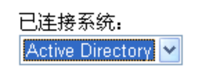
2 选择现有驱动程序所驻留的驱动程序集，然后单击 《下一步》。



3 在显示的驱动程序配置列表中选择 《Password Synchronization 2.0 策略》，然后单击《下一步》。



4 从下拉列表中选择 *Active Directory* 。



5 选择 *Active Directory* 作为已连接系统，然后单击 《下一步》。

6 对于有关驱动程序和已连接系统的功能的三个提示，回答 《是》。

- 已连接系统是否能够向 Identity Manager 提供口令。
- 已连接系统是否能够从 Identity Manager 接受口令
- 已连接系统是否能够检查某个口令，以确定该口令是否与 Identity Manager 中的口令匹配。

7 单击 《下一步》，然后选择更新有关驱动程序的所有项目。

此选项可指定口令同步必需的驱动程序清单、全局配置值 (GCVs) 和口令策略。

驱动程序清单和 GCV 将重写已存在的任何值，但由于这些类型的驱动程序参数是 Identity Manager 中的新参数，因此，不应该会重写任何现有值。

口令策略不会重写任何现有策略对象。只会将这些策略对象添加到驱动程序对象。

如果没有要保存的驱动程序清单或 GCV 值，请选择该驱动程序的、名称为 《只更新选定的策略》的选项，然后选中所有策略的复选框。此选项将导入口令策略，但是不更改驱动程序清单或 GCV。

8 单击 《下一步》，然后单击 《完成》以完成向导。

至此，驱动程序对象下方已创建用作策略对象的新策略。但是，这些新策略还不是驱动程序配置的一部分。要链接这些策略，必须在 《订购者》和 《发布者》通道上，将每一个策略手动插入到驱动程序配置中的正确位置。

9 将每个新策略插入到现有驱动程序配置中的正确位置。

如果策略集具有多个策略，请确保最后列出这些口令同步策略。

有关策略列表以及这些策略插入的位置，请参见 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）中的 《Policies Required in the Driver Configuration》（驱动程序配置中所需的策略）。

针对每个策略重复步骤 9a 至 9e。

9a 单击 《Identity Manager》 > 《Identity Manager 概述》 > ，然后选择所更新的驱动程序的驱动程序集。

9b 单击刚刚更新的驱动程序。

将打开一个页，其中显示驱动程序配置的图形表示形式。

9c 单击需要将其中一个新策略添加到的位置的图标。

9d 单击 《插入》以添加新策略。

在显示的 《插入》页中单击 《使用现有策略》，通过浏览找到新策略对象，然后单击 《确定》。

9e 在列表中，如果任何一个新策略具有多个策略，请使用箭头按钮 将新策略移到列表中的正确位置。

确保策略遵循 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）的 《Policies Required in the Driver Configuration》（驱动程序配置中所需的策略）中列出的顺序。

10 更改驱动程序的过滤器，以允许同步 nspmDistributionPassword 特性。

只对 《订购者》通道启用通知。将 《发布者》通道设置为 《忽略》。

11 必要时设置 SSL。

"解决安全问题"在第 15 页 中包含了指导。

驱动程序在 Active Directory （《订购者》通道）中设置口令的功能需要下列其中一个条件提供安全的连接：

- 运行驱动程序的计算机与域控制器是同一台计算机。
- 运行驱动程序的计算机与域控制器在同一个域中。
- 对于不在域中的计算机，需要在该计算机与域控制器之间设置 《简单》方法和 SSL。仅当使用 《协商》鉴定机制时，双向口令同步才可用。

  有关指导，请参考 Microsoft 文档，例如 《在域控制器上配置数字证书 (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp)》。

12 如果需要已连接系统向 Identity Manager 提供用户口令，请安装新的口令同步过滤器，并对其进行配置。请参见 "设置口令同步过滤器"在第 65 页 。

至此，驱动程序已具有新的驱动程序 Shim、 Identity Manager 格式，以及支持口令同步所必需的其它部分：驱动程序清单、 GCV、口令同步策略和过滤器。现在，可以使用 iManager 中的口令同步界面，指定希望口令如何流向已连接系统，以及如何从已连接系统流出。

13 使用驱动程序的口令策略和口令同步设置，设置需要使用的口令同步方案。

请参见 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）中的 《Implementing Password Synchronization》（实现口令同步）。

14 针对希望其参与口令同步的所有驱动程序重复步骤 1 至 14。

7.5 设置口令同步过滤器

要使驱动程序只在一台 Windows 计算机上运行，需要对该驱动程序进行配置。

但是，安装和配置驱动程序后，请针对其它每个域控制器执行下列操作：

1. 安装口令过滤器 （pwfilter.dll 文件）。
2. 配置注册表以截取口令，以便能够将口令发送到 Identity Manager。

启动域控制器时，将自动启动口令过滤器。过滤器使用 Windows 客户机截取用户所做的口令更改，再加密更改，然后将这些更改发送到驱动程序，以更新 Identity Manager 数据储存。

注释 **:** 有关配置口令同步的信息，请参见 *《Novell Identity Manager 3.0 Administration Guide》*（Novell Identity Manager 3.0 管理指南）中的 《Implementing Password Synchronization》（实现口令同步）。

为简化口令过滤器的设置和管理，可以在安装驱动程序时，将一个 Identity Manager PassSync 实用程序添加到控制面板。根据您是否允许对域控制器上的注册表进行远程访问，该实用程序提供用于设置口令过滤器的两个选项：

- 如果允许对注册表进行远程访问： 从计划在其上运行驱动程序的单台计算机上，使用 Identity Manager PassSync 实用程序为所有域控制器配置口令过滤器。

  此方法允许您从一个位置配置所有域控制器。

  如果从一台计算机配置所有域控制器，在设置期间， Identity Manager PassSync 实用程序可提供下列功能对您进行帮助：
  - 允许您指定希望哪个域参与口令同步。
  - 自动发现域的所有域控制器。
  - 允许您在每个域控制器上远程安装 pwfilter.dll。
  - 自动更新运行驱动程序的计算机上的注册表，以及每个域控制器上的注册表。
  - 允许您查看每个域控制器上的过滤器的状态。
  - 允许您远程重引导域控制器。

    由于截取口令更改的过滤器是启动域控制器时将会启动的 DLL 文件，因此，首次添加用于口令同步的域时，该功能是必要的。

  请参见 “从一台计算机为所有域控制器配置口令过滤器”在第 66 页 。

- 如果不允许对注册表进行远程访问：针对每个域控制器单独设置口令过滤器。要执行此操作，请转至每个域控制器，安装驱动程序文件以获得 Identity Manager PassSync 实用程序，然后在每台计算机上使用该实用程序安装口令过滤器，并更新注册表。

  请参见 “针对每个域控制器单独配置口令过滤器” 在第 69 页 。

7.5.1 从一台计算机为所有域控制器配置口令过滤器

此过程说明如何针对每个域控制器安装和配置口令过滤器 （所有操作在运行驱动程序的同一台计算机上完成）。

如果允许对注册表进行远程访问，请使用该方法。

由于设置过滤器需要重引导域控制器，因此可能需要在数小时之后执行此过程，或者一次只重引导一个域控制器。如果域具有多个域控制器，那么请记住，要在其上运行口令同步的每个域控制器必须安装了过滤器，并且必须被重引导。

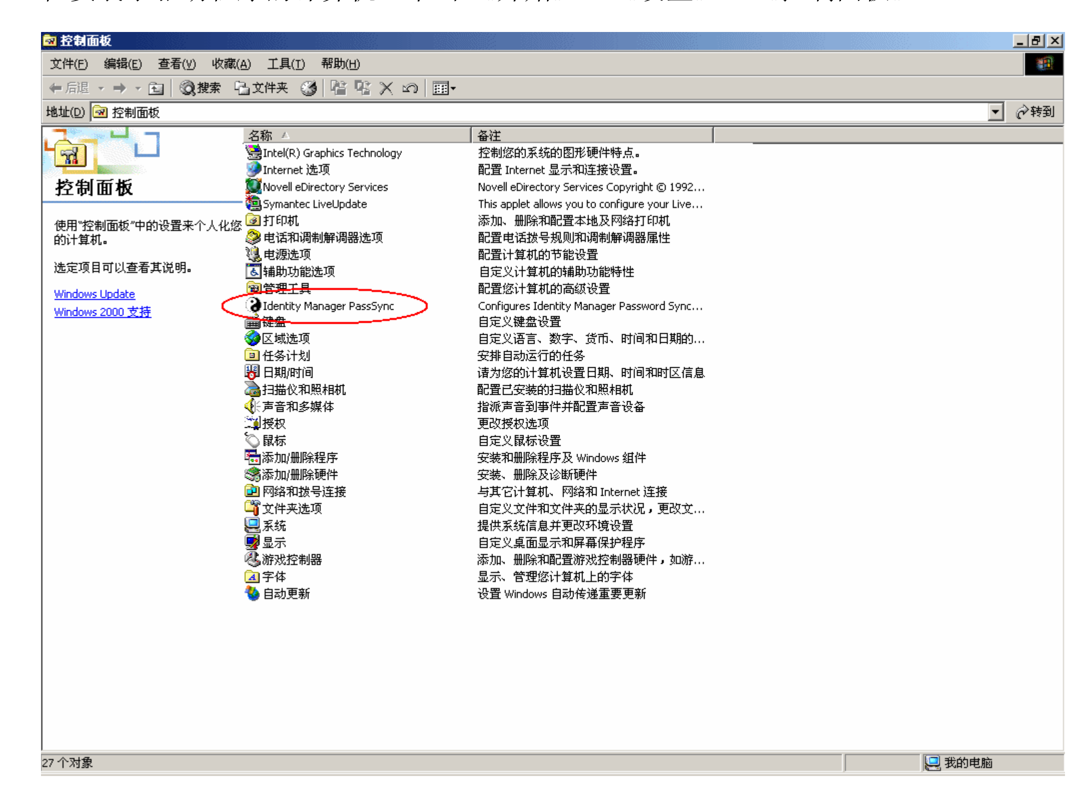
1 确认可以访问域控制器上的端口 135 （RPC 终点映射程序），并且可以访问 Identity Manager Driver for Active Directory 在其上进行配置以便能够运行的计算机上的该端口。

   如果使用的是 TCP 上的 NetBIOS，则还需要下列端口：

   - 137: NetBIOS 名称服务
   - 138: NetBIOS 数据报文服务
   - 139: NetBIOS 会话服务

   防火墙可以防止对端口进行远程访问。

2 在安装了驱动程序的计算机上单击 《开始》 > 《设置》 > 《控制面板》。



3 双击 *Identity Manager PassSync*。

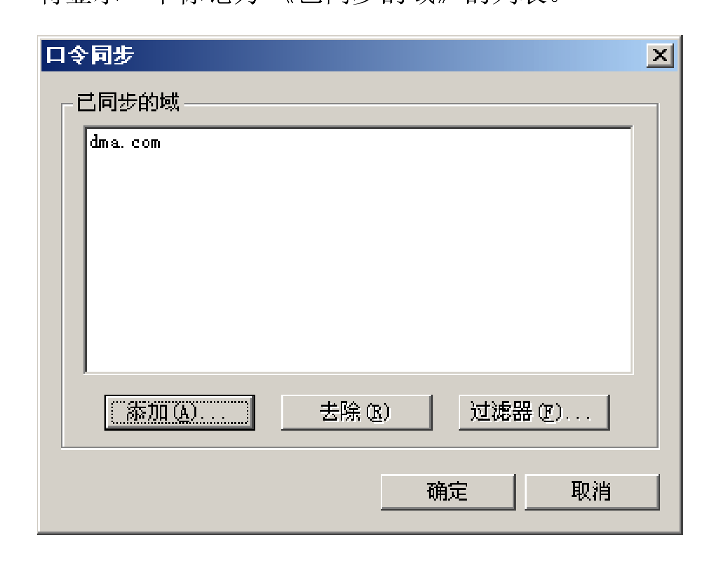
首次打开该实用程序时，它会询问这是否为安装了 Identity Manager 驱动程序的计算机。



完成配置后，除非从列表中去除该域，否则不会再次显示该提示。

4 单击 《是》。

将显示一个标记为 《已同步的域》的列表。



5 要添加一个希望其参与口令同步的域，请单击 《添加》。

将显示 《添加域》对话框。

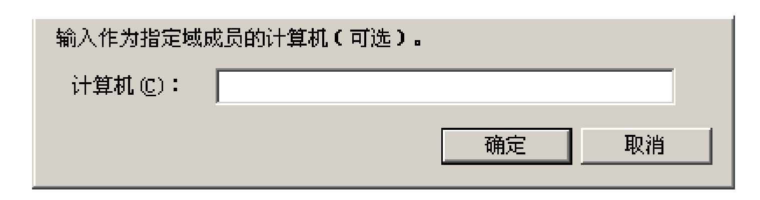


6 指定或选择要添加的域名。



下拉列表将显示已知的域。

7 （可选操作）指定域中的计算机。



如果将 《计算机》编辑框留空， PassSync 将查询本地计算机。因此，如果在域控制器上运行 PassSync，则不需要输入名称。PassSync 将查询本地计算机 （在此情况下为域控制器），并 （从数据库）获取域中所有域控制器的列表。

如果不是在域控制器上执行安装，请输入域中的、并且能够与域控制器通讯的计算机的名称。

如果收到一条错误讯息，指明 PassSync 无法找到域，则请输入另一个名称。

8 确定是否使用域的 DNS 名称。

DNS 名称提供更高级的鉴定和功能，用于以更可靠的方式发现大型安装中的域。但是，选择取决于环境。

9 使用管理员权限登录。

Identity Manager PassSync 实用程序将发现该域的所有域控制器，并在每个域控制器上安装 pwfilter.dll。它还将更新运行了驱动程序的计算机上的注册表，以及每个域控制器上的注册表。这可能要花几分钟时间。

在重引导域控制器之前，pwfilter.dll 不截取口令更改。可使用 Identity Manager PassSync 实用程序查看所有域控制器的列表，以及这些域控制器上的过滤器的状态。还可以从该实用程序内部重引导域控制器。

10 在列表中单击域名，然后单击 《过滤器》。

实用程序将显示所有域控制器的名称，以及每个域控制器上的过滤器的状态。

每个域控制器的状态应指明该域控制器需要重引导。但是，实用程序可能需要几分钟时间才能完成其自动任务，同时，状态可能会提示 《未知》。



11 重引导每个域控制器。

可以选择在对环境有利的时间重引导这些域控制器。只是请记住，在重引导每个域控制器之前，口令同步不能完全正常地运行。

12 如果所有域控制器的状态都提示 《正在运行》，请测试口令同步以确认域控制器是否已运行。

13 要添加其它域，请单击 《确定》返回到域列表，然后重复步骤 6 至步骤 12。

7.5.2 针对每个域控制器单独配置口令过滤器

本节所述的过程说明如何针对每个域控制器一次性安装和配置口令过滤器。

如果不允许对注册表进行远程访问，请使用该方法。

在此过程中，需要安装驱动程序以获得 Identity Manager PassSync 实用程序。然后将使用该实用程序安装 pwfilter.dll 文件，指定要使用的端口，并指定由哪台主机运行 Identity Manager Driver for Active Directory。

由于设置过滤器需要重引导域控制器，因此可能需要在数小时之后执行此过程，或者一次只重引导一个域控制器。如果域具有多个域控制器，那么请记住，要在其上运行口令同步的每个域控制器必须安装了过滤器，并且必须被重引导。

1 确认下列端口在域控制器上可用，并且在 Identity Manager Driver for Active Directory 在其上进行配置以能够运行的计算机上可用：

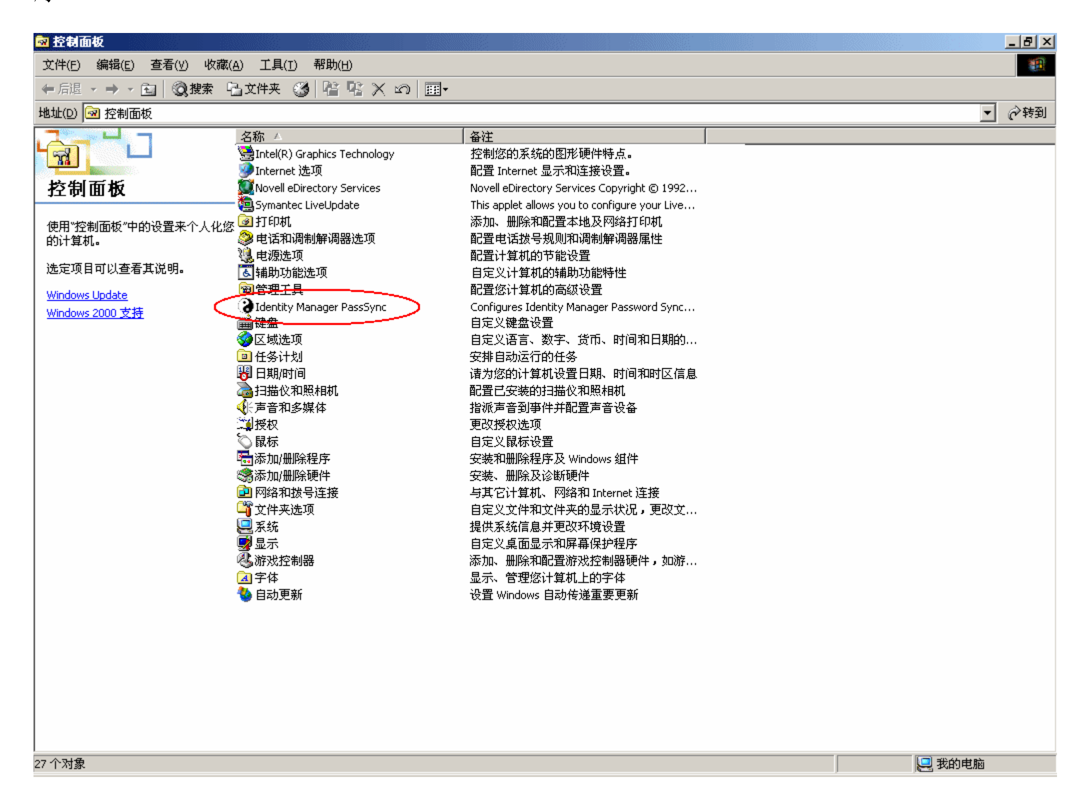
- 135: RPC 终点映射程序

- 137: NetBIOS 名称服务
- 138: NetBIOS 数据报文服务
- 139: NetBIOS 会话服务

2 在域控制器上，使用 Identity Manager 安装来安装 Identity Manager Driver for Active Directory （仅安装此项）。

安装驱动程序即可安装 Identity Manager PassSync 实用程序。

3 单击 《开始》 > 《设置》 > 《控制面板》，然后找到 Identity Manager PassSync 实用程序。



4 双击 *Identity Manager PassSync*。

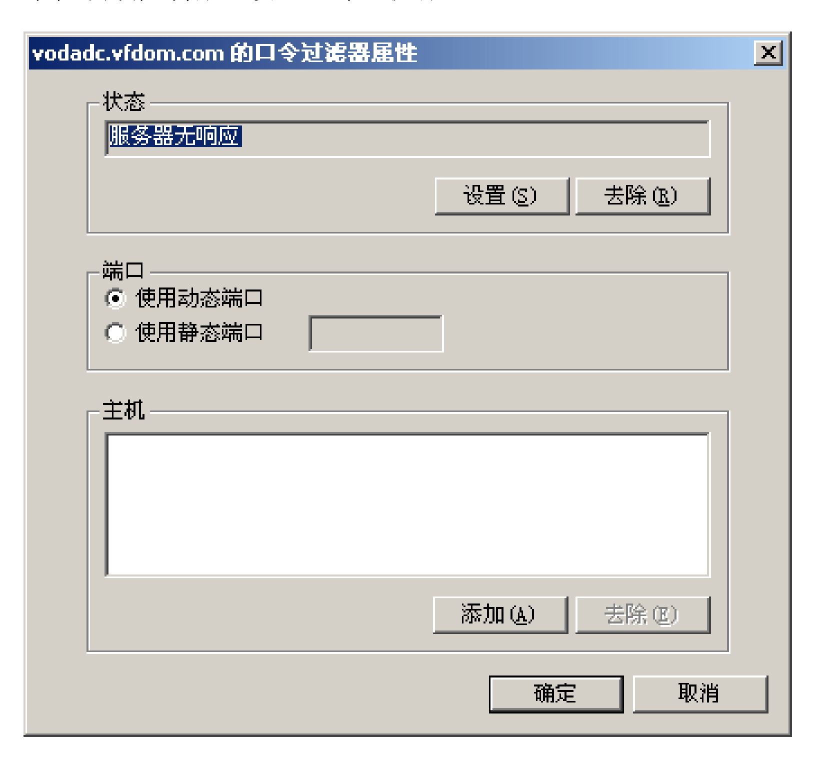
首次打开该实用程序时，它会询问这是否为安装了 Identity Manager 驱动程序的计算机。



5 单击 《否》。

完成配置后，除非在 《口令过滤器属性》对话框中，使用 《去除》按钮去除口令过滤器，否则不会再次显示该提示。

单击 《否》后，将显示 《口令过滤器属性》对话框，其中显示一条状态讯息，指明尚未在该域控制器上设置口令过滤器。

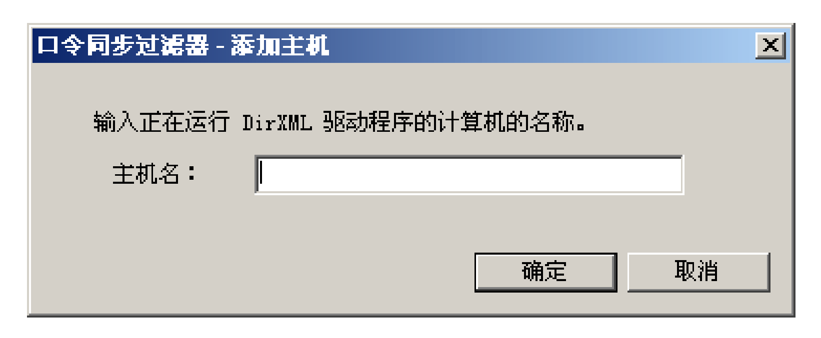


6 单击 《设置》按钮安装口令过滤器 pwfilter.dll。

7 对于端口设置，请指定是使用动态端口还是使用静态端口。

仅当已确定以不同于默认方式的方式为域控制器配置远程过程调用 (RPC) 时，才使用静态端口选项。

8 指定 Identity Manager 驱动程序的位置，单击 《添加》按钮，指定运行 《口令同步过滤器 - 添加主机》对话框中的 Identity Manager 驱动程序的计算机的主机名，然后单击《确定》。



该步骤是必需的，这样口令过滤器就知道将口令更改发送到何处。口令过滤器将截取口令更改，并且必须将这些更改发送到 Identity Manager 驱动程序，以更新 Identity Manager 数据储存。

9 在 《口令过滤器属性》对话框中单击 《确定》。

10 重引导域控制器以完成口令过滤器的安装。

可以选择在对环境有利的时间执行重引导。只是请记住，在每个域控制器上安装口令过滤器且重引导每个域控制器之前，口令同步不能完全正常地运行。

完成安装并且重引导域控制器后，只要启动域控制器，就会自动装载口令过滤器。

11 通过单击 《开始》>《设置》>《控制面板》，然后双击 Identity Manager PassSync 实用程序，再次检查口令过滤器的状态。

确认状态是否提示为 《正在运行》。

12 针对希望其参与口令同步的每个域控制器，重复步骤 2 至步骤 11。

13 如果所有域控制器的状态都提示 《正在运行》，请测试口令同步以确认域控制器是否已运行。

7.6 失败后重试同步

已增强驱动程序和口令过滤器，以改善失败后重试口令同步的方式。

7.6.1 添加或修改事件之后重试

如果从 Active Directory 发送的口令更改没有在 Identity Vault 中成功地完成，驱动程序将超速缓存该口令。在口令所属的用户发生 《添加》或 《修改》事件之前，不会再次重试该口令。 （以前，按每个巡回检测间隔重试这些保存的口令。）

当驱动程序巡回检测 Active Directory 中的更改时，驱动程序将收到用户的 《添加》或 《修改》事件。对于每个用户 《添加》或 《修改》事件，驱动程序将检查是否为此新用户保存了口令。如果未保存，驱动程序会以修改用户事件的形式将口令发送到 Identity Vault。

如果设置了口令同步，以便在口令同步失败时，向用户发送电子邮件讯息，则此增强会将用户可能接收到的电子邮件数减至最少。

7.6.2 口令失效时间

添加了一个名称为 《Password Expiration Time》的参数。如果第一次尝试同步时不成功，可使用该参数确定需要用多长的时间来保存特定用户的口令。驱动程序将保存口令，直到在 Identity Vault 中成功更改该口令，或直到耗尽了 Password Expiration Time。

导入样本驱动程序配置时，系统将提示您指定失效时间。如果不指定时间，或者时间 （间隔字段）包含无效字符，则使用默认设置 60 分钟。如果指定的时间小于指定的巡回检测间隔的三倍，则驱动程序会将时间更改为巡回检测间隔的三倍。

请将该值设置到大小足以处理所存在的任何口令临时代办事项。如果执行的是大批量更改，请将超时设置到大小足以处理所有的更改。经验法则是每个口令允许一秒钟。例如，要同步 18,000 个口令，则允许 300 分钟 （18,000 个口令除以 60 秒）。

如果设置为 -1，则不限时。尽管此设置可以处理大批量更改，但它会导致出现问题。例如，因为没有对帐户进行关联，所以永远无法对口令进行同步。因此，这样的口令将永远保留在系统中。如果存在许多类似的情况，则会导致系统需要为未同步口令保留较大的库存。

与口令失效时间相关的方案

在 《发布者》通道上，口令同步可能在 《添加》事件之前发生。驱动程序紧接在 《添加》事件之后重试。

方案：无影响

在 Active Directory 中创建了一个带有口令的新用户。过滤器立即将新口令发送到驱动程序。但是，驱动程序仍收到该用户的 《添加》事件，因为该事件已在巡回检测间隔之间发生。由于驱动程序尚未在 Identity Vault 中创建用户，因此这第一次口令同步尝试不成功。驱动程序将超速缓存口令。

在下一个巡回检测间隔，驱动程序将收到新用户的 《添加用户》事件。驱动程序还将检查是否为此新用户超速缓存了口令。驱动程序会将 《添加用户》事件发送到 Identity Vault，同时发送 《修改用户》事件以同步口令。

在这种情况下，口令同步只会延迟一个巡回检测间隔。

Password Expiration Time 参数在此场合下不产生影响。

方案：增加失效时间

在 Active Directory 中创建了一个带有口令的新用户。但是，此用户信息不符合 Active Directory 驱动程序的创建策略的要求。

例如，可能创建规则需要全名，并且必需的信息已丢失。与 《无影响》示例一样，过滤器会立即将口令更改发送到驱动程序。但是，在 Identity Vault 中，口令更改的第一次尝试不成功，因为用户尚不存在。驱动程序将超速缓存口令。

但是，在这种情况下，即使驱动程序巡回检测 Active Directory 中的更改，并且可发现新用户，驱动程序也不能创建新用户，因为此用户信息不符合创建策略的要求。

创建新用户和同步口令将会延迟，直到在 Active Directory 中添加所有用户信息以满足创建策略。然后，驱动程序将在 Identity Vault 中添加新用户，检查是否为此新用户超速缓存了口令，再发送一个 《修改用户》事件以同步口令。

仅当时间间隔在 Active Directory 中的用户信息符合创建策略的要求之前耗尽时， Password Expiration Time 参数才影响此方案。如果 《添加》事件在口令失效后发生，并且驱动程序没有为该用户超速缓存口令，则不能发生同步。由于驱动程序没有超速缓存的口令，因此驱动程序将使用口令策略中的默认口令。

用户在 Active Directory 或 Identity Vault 中更改口令后，该口令将被同步。

如果设置了口令同步以实现口令的双向流动，那么在 Identity Vault 中执行口令更改后，还可以将口令从 Identity Vault 同步到 Active Directory。

如果创建策略受到限制，并且它通常需要一天以上的时间在 Active Directory 中完成新用户的信息，则可能需要相应地增大 Password Expiration Time 参数间隔。然后，驱动程序将超速缓存口令，直到最终在 Identity Vault 中创建了用户。

方案：永不符合要求

在 Active Directory 中创建了一个带有口令的用户。但是，此用户永远不能符合 Active Directory 驱动程序的创建策略的准则。

例如，可能 Active Directory 中的新用户具有指明用户是合同工的说明，而创建策略阻止为合同工创建用户对象，因为业务策略规定，未计划让合同工在 Identity Vault 中拥有相应的用户帐户。与上一个示例一样，过滤器将立即发送口令更改，但是第一次口令同步尝试将不会成功。驱动程序将超速缓存口令。

在这种情况下，永远都不能在 Identity Vault 中创建相应的用户帐户。因此，驱动程序永远都不会同步超速缓存的口令。经过口令失效时间后，驱动程序将从超速缓存中去除用户口令。

方案：电子邮件通知

Markus 有一个 Active Directory 帐户和相应的 Identity Vault 帐户。他更改了他的 Active Directory 口令，该口令包含六个字符。但是，该口令不符合管理员在 eDirectory 中创建的口令策略指定的最少八个字符的要求。将配置口令同步以拒绝不符合策略的口令，同时向 Markus 发送一封通知电子邮件，指明口令同步失败。驱动程序将超速缓存口令，并且仅当更改了 Active Directory 中的用户对象后，才重试该口令。

在这种情况下，更改口令后不久， Markus 将收到一封电子邮件，指明口令同步未成功。驱动程序每次重试口令后， Markus 都会收到相同的电子邮件讯息。

如果 Markus 将 Active Directory 中的口令更改为符合口令策略的口令，则驱动程序可以成功地将新口令同步到 Identity Vault。

如果 Markus 不将该口令更改为符合要求的口令，则口令同步永远不能成功。经过口令失效时间后，驱动程序将删除超速缓存的口令，且不再重试该口令。

查错

8

8.1 不能从发布者或订购者通道同步更改

要同步 Active Directory 中的更改，必须为 Identity Manager 驱动程序使用的帐户设置适当的权限。有关必需权限的信息，请参见 "创建管理帐户"在第 19 页 。

如果使用默认策略，还必须符合创建策略、匹配策略和布局策略的要求。有关默认策略的要求的信息，请参见 "策略"在第 8 页 。

特性 dirxml-uACLockout 不能在 《发布者》通道上同步。

8.2 使用超出有效 NT 登录名范围的字符

默认的订购者创建策略根据 Identity Vault 中的帐户的相对判别名生成 NT 登录名 （又称《sAMAccountName》和 《Windows 2000 以前版本的登录名》）。NT 登录名使用 ASCII 字符集的子集。默认策略在 Active Directory 中创建对象之前，将去除超出有效范围的任何字符。

如果策略不满足公司的业务规则，则可以在导入后更改策略。使用超出传统的 ASCII 字符集范围的 Identity Vault 帐户名的业务部门应特别注意此策略。

8.3 同步 c、 co 和 countryCode 特性

使用 Active Directory 管理控制台选择用户的国家 / 地区时，需要设置三个特性：

表 ***8-1*** 国家 / 地区的特性

特性	说明
c	包含 ISO 定义的两字符国家代码。
co	包含国家 / 地区的较长的名称。
countryCode	包含代表国家 / 地区的数字值 （该值也由 ISO 定义）。

由于 ISO 定义的数字型国家代码计划由不能处理字母字符的应用程序使用，因此，默认情况下， Identity Vault 中的纲要包括 c 和 co，但不包括 countryCode。

Identity Manager 能够映射 c 和 co。如果向 eDirectory™ 纲要添加了类似的特性，则它还可以映射 countryCode。

Active Directory 的管理控制台将尝试使这三个特性保持同步，以便在控制台上设置国家 / 地区时，所有三个特性都具有相应值。如果通过 Identity Manager 设置特性，某些管理员可能需要与此相类似的行为。例如，可能需要配置驱动程序，这样，即使过滤器中只有 c，在《订购者》通道上发送了 c 的更改后，同样会设置 co 和 countryCode。

8.4 同步操作特性

操作特性是指由包含特殊操作信息的 LDAP 服务器维护的特性。操作特性是只读的。不能同步或更改这些特性。

8.5 Windows 2003 上的口令复杂性

口令必须符合口令策略指定的准则。

Windows 2000/2003 口令策略中的复杂性和要求与 eDirectory 中的复杂性和要求有所不同。

如果计划使用口令同步，请创建并使用与 Active Directory 和 eDirectory™ 中的复杂性规则都匹配的口令。否则，口令将会失败。

提示 : 为两个系统创建尽可能类似的口令策略。在实验室环境中，安装 Active Directory 驱动程序之前，请对 Windows 2003 服务器禁用强口令功能。Active Directory 驱动程序正常运行后，确保 eDirectory 和 Active Directory 中使用的口令符合这两个系统的复杂性规则。然后对 Windows 2003 服务器重新启用强口令功能。

有关查错提示，请参见 TID 10083320 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10083320.htm)。

8.6 错误讯息 LDAP_SERVER_DOWN

错误代码 LDAP_SERVER_DOWN 通常表示驱动程序无法打开为同步配置的 Active Directory 域控制器上的 LDAP 端口。有多种原因会导致发生此情况。

- 驱动程序鉴定环境中指定的服务器不正确。鉴定环境应保存用于同步的域控制器的 DNS 名称或 IP 地址。如果将参数留空，驱动程序将尝试与运行驱动程序 Shim 的计算机连接 （运行 IDM 的同一台服务器，或承载远程装载程序的服务器）。

- 对鉴定环境使用了 IP 地址，并且禁止对 Active Directory 进行非 Kerberos 鉴定。Kerberos 要求对鉴定环境使用 DNS 名称。

  驱动程序 Shim 只能使用 Windows 2000 以前版本登录方法或简单联结进行鉴定。如果在网络上禁用 NTLM、 NTLM2 和简单联结，则可能会收到 LDAP_SERVER_DOWN 讯息。
- 配置了驱动程序，以便对 Active Directory 使用 SSL 连接。该讯息表示导入到驱动程序 Shim 服务器的证书存在某些问题 （或根本没有导入证书）。

8.7 口令同步的提示

建议在同步口令时使用安全的连接。下列两者之间的连接很容易受到攻击：

- Metadirectory 引擎和远程装载程序
- 远程装载程序和 Active Directory

  仅当从连接到的域控制器远程运行远程装载程序时，此情况才属实。
- 不使用远程装载程序时的 Metadirectory 引擎和 Active Directory

  仅当域控制器不在该计算机上时，此情况才属实。

通过执行下列其中一项或多项操作来创建一个安全的连接：

- 配置 Metadirectory 引擎和远程装载程序之间的 SSL
- 在域控制器上运行远程装载程序
- 配置驱动程序 Shim 和 Active Directory 之间的 SSL

  如果在连接到的域控制器上运行驱动程序，则此情况不应用。

驱动程序 Shim 不在域控制器上运行时，要使口令同步运行，必须配置 SSL。

8.7.1 提供初始口令

最初创建用户时，如果看到有关口令不符合要求的错误，则需要检查口令策略。

例如， Active Directory 驱动程序在 Identity Vault 中创建用户对象时，您可能需要 Active Directory 驱动程序提供某个用户的初始口令。创建用户后，驱动程序 Shim 将创建用户，然后设置口令。

由于添加用户与设置口令是分开执行的，因此，此示例中的新用户将会接收默认口令，即使只是暂时使用默认口令。Active Directory 驱动程序在添加用户后会立即发送口令，因此口令很快就会更新。

如果默认口令不符合用户的 eDirectory 口令策略，则会显示错误。例如，如果使用用户姓氏创建的默认口令太短，以致于不符合口令策略，则会显示指明口令太短的 -216 错误。但是，如果 Active Directory 驱动程序随即发送了一个符合策略的初始口令，则此情况很快就会得到矫正。

如果希望创建用户对象的已连接系统提供初始口令，则无论使用哪个驱动程序，都请考虑执行下列操作之一：

- 在 《发布者》通道上更改创建默认口令的策略，以便默认口令符合在 Identity Vault 中为组织定义的口令策略 （这些策略是在口令管理中使用 《管理口令策略》选项创建的）。如果初始口令来自授权应用程序，则该口令将替换默认口令。

最好使用该选项。建议保留默认口令的策略，以保持系统中较高的安全级别。

- 在 《发布者》通道上去除创建默认口令的策略。在样本配置中，此策略在命令转换策略集中提供。允许在 eDirectory 中添加不带口令的用户。此选项的假定条件是，新建的用户对象的口令最终将会通过 《发布者》通道，因此这个不带口令的用户对象只是短时间存在。

如果初始口令不是由添加事件产生的，而是由后续事件产生的，则这些措施尤其重要。

8.8 在哪里设置 SSL 参数

驱动程序配置中的 SSL 参数用于 Active Directory 驱动程序和 Active Directory 之间的 SSL。它不是用于 Metadirectory 引擎和远程装载程序之间的 SSL。请参见 "加密"在第 16 页 。

8.9 在订购者通道上执行用户添加操作后禁用了 Active Directory 帐户

默认配置会将 Identity Vault Logon Disabled 特性映射到 Active Directory 中 userAccountControl 特性的 dirxml-uACAccountDisable 位。订购者添加操作可能会将 Logon Disabled 设置为假 （已启用帐户），但是添加操作的发布者回送将报告 Logon Disabled 为真 （已禁用帐户）。

此外，在 Active Directory 中检查对象时可能会显示禁用了帐户。发生这种情况的一部分原因与驱动程序在 Active Directory 中创建对象的方式有关，另一部分原因与驱动程序和 Active Directory 本身之间的策略不匹配有关。

8.9.1 在 Active Directory 用户和计算机中禁用了帐户

供应周期完成后，如果 Active Directory 中的帐户保持为禁用状态，则可能是为驱动程序配置的策略与 Active Directory 实施的策略不匹配。

以必需口令策略为例。如果用户添加操作包含无效口令 （或根本没有口令），则应该禁用在 Active Directory 中创建的帐户。但是 Active Directory 可能在驱动程序不知情的情况下，设置 userAccountControl 中的 dirxml-uACPasswordNotRequired 位。

有意思的是，如果添加操作不包含 dirxml-uACPasswordNotRequired 的策略，则这种情况会导致添加操作的登录启用操作失败。因此，帐户将保持为禁用状态。

以后 （也可能是立即 - 由于合并操作），驱动程序可能会通过将 Logon Disabled 设置为假，尝试再次启用帐户。如果要覆盖 Active Directory 策略，并且确保帐户始终需要一个口令，则只要 Logon Disabled 在 《订购者》通道上发生更改，就应该将 dirxml-uACPasswordNotRequired 设置为假。

8.10 将父邮箱移动到子域

如果通过更改用户的 homeMDB 特性将父邮箱移动到子域中的邮箱储存，驱动程序将无法执行移动。返回的错误代码为 0x80072030。

执行域间移动时会发生此错误。不支持将 Exchange 父邮箱移动到子域。

8.11 恢复 Active Directory

如果需要恢复整个 Active Directory 或恢复其一部分，驱动程序可能会选择临时事件，并对 Identity Vault 执行不需要的操作。要安全恢复，请在恢复过程中暂时禁用驱动程序，然后使 Identity Vault 重新与 Active Directory 同步。

1 禁用驱动程序。
2 在 Identity Vault 中删除驱动程序对象上的 Dirxml-DriverStorage 特性。
3 恢复 Active Directory。
4 将 Active Directory 驱动程序设置为手动启动或自动启动。
5 启动驱动程序。
6 重新迁移以查找不关联的对象。

8.12 将驱动程序移动到不同的域控制器

可通过更改驱动程序的 Authentication Context 参数，配置驱动程序，以便与不同的域控制器同步。重启动驱动程序时，该驱动程序用来跟踪 Active Directory 中的更改的状态信息将会无效，同时 Active Directory 可能会重放大量的旧事件来使状态返回到当前时间。

在更新 Authentication Context 时去除驱动程序的状态信息可避免此重放操作：

1 停止驱动程序。
2 在 Identity Vault 中删除驱动程序对象上的 Dirxml-DriverStorage 特性。
3 更新 Authentication Context 参数。
4 启动驱动程序。

   这会导致 Identity Vault 中的关联对象发生重新同步。
5 重新迁移以查找 Active Directory 中不关联的对象。

8.13 从 Active Directory 迁移

从 Active Directory 迁移到 Identity Vault 时，需要注意 Active Directory 服务器上的对象包容、DN 参照和搜索限制。处理包容的一般策略是先迁移树枝，然后迁移可能是组成员的对象（包括用户对象），最后迁移组。如果要迁移中等数量的对象，则需要调整策略，以处理在 Active Directory 服务器上配置的 LDAP 搜索限制。可以在 LDAP 服务器上更改限制，或者调整迁移，以便每次只获取对象的一个子集 （例如，一个树枝接一个树枝地迁移，或者迁移以 《A》、《B》等开头的对象）。

8.14 设置 LDAP 服务器搜索限制

下面是一个终止会话，显示如何使用 NTDSUTIL.EXE 更改域控制器上的 LDAP 搜索参数。只需要更改在迁移的持续时间内，用于 IDM 同步的域控制器上的这些设置。写下当前配置值，并在完成迁移后运行 NTDSUTIL.EXE，以恢复原始值。可以在任何成员服务器上运行 NTDSUTIL.EXE。

1 在命令提示符下键入 ntdsutil。
2 键入 LDAP Policies，然后按 Enter 键。
3 键入 Connections，然后按 Enter 键。

4 键入 Connect to domain *domain_name*，然后按 Enter 键。

5 键入 Connect to server *server_name*，然后按 Enter 键。

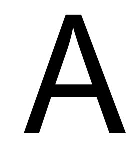
6 键入 Quit，然后按 Enter 键。

7 键入 Show Values，然后按 Enter 键。

```
C:\>ntdsutil ntdsutil: LDAP Policies ldap policy: Connections server
connections: Connect to domain raptor Binding to \\raptor1.raptor.lab
... Connected to \\raptor1.raptor.lab using credentials of locally
logged on user. server connections: Connect to server raptor1
Disconnecting from \\raptor1.raptor.lab... Binding to raptor1 ...
Connected to raptor1 using credentials of locally logged on user.
server connections: Quit ldap policy: Show Values

Policy                      Current(New) MaxPoolThreads
4 MaxDatagramRecv                  4096 MaxReceiveBuffer
10485760 InitRecvTimeout               120 MaxConnections
5000 MaxConnIdleTime                 900 MaxPageSize
1000 MaxQueryDuration                120 MaxTempTableSize
10000 MaxResultSetSize            262144 MaxNotificationPerConn
5 MaxValRange                     1500ldap policy: set MaxQueryDuration
to 1200 ldap policy: set MaxResultSetSize to 6000000 ldap policy:
Commit Changes ldap policy: Quit ntdsutil: Quit Disconnecting from
raptor1...C:\>
```

更改对 CN=Deleted Objects 树枝的许可权限



删除了一个 Active Directory 对象后，将在指定的时间内保留该对象的一小部分，以便复制更改的其它域控制器知道发生了删除。默认情况下，只有 System 帐户和 Administrators 组的成员才能查看该树枝的内容。本节说明如何修改对 CN=Deleted Objects 树枝的许可权限。

如果企业应用程序或服务使用非 System 帐户或非 Admin 帐户联结到 Active Directory，并且它们会巡回检测目录更改，则可能需要更改对 Deleted Objects 树枝的许可权限。

此过程需要 Active Directory 应用程序方式 (ADAM) 包中的 dscals.exe。此版本是从 Windows Server 2003 支持工具中的版本升级而来的，它现在支持必需的功能。ADAM 管理工具受 Windows XP Professional、 Windows Server 2003 Standard Edition、 Windows Server 2003 Enterprise Edition 和 Windows Server 2003 Datacenter Edition 的支持。

要获取和安装 ADAM 管理工具，请执行下列操作：

1. 在 ADAM 万维网网页 (http://www.microsoft.com/downloads/details.aspx?FamilyId=9688F8B9-1034-4EF6-A3E5-2A2A57B5C8E4&displaylang=en) 上，下载 ADAM 零售包。
2. 双击下载的文件，然后提供档案解压缩到的目录。
3. 双击 adamsetup.exe，启动 Active Directory 应用程序方式设置向导，然后单击 《下一步》。
4. 查看并接受许可条款，然后单击 《下一步》。
5. 只选择 ADAM 管理工具，然后单击 《下一步》。
6. 查看选择，然后单击 《下一步》。
7. 结束设置后，单击 《完成》。

安装 ADAM 管理工具后，修改对 CN=Deleted Objects 树枝的许可权限：

1. 使用作为 Domain Admins 组成员的用户帐户登录。
2. 单击 《开始》 > 《所有程序》 > 《ADAM》 > 《ADAM 工具命令提示符》。
3. 在命令提示符下，输入以下命令：

   ```
   dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /takeownership
   ```

   替代您自己的域的 Deleted Objects 树枝的判别名。

   林中的每个域都将有其自身的 Deleted Objects 树枝。

   应显示以下输出：

   ```
   Owner: Contoso\Domain Admins Group: NT AUTHORITY\SYSTEM Access
   list: {This object is protected from inheriting permissions from
   the parent} Allow BUILTIN\Administrators  SPECIAL ACCESS LIST
   CONTENTS READ PROPERTY Allow NT AUTHORITY\SYSTEM    SPECIAL ACCESS
   DELETE READ PERMISSONS WRITE PERMISSIONS CHANGE OWNERSHIP CREATE
   ```

```
CHILD DELETE CHILD LIST CONTENTS WRITE SELF WRITE PROPERTY READ
PROPERTY The command completed successfully
```

4 要授予安全主体许可权限以查看 CN=Deleted Objects 树枝中的对象，请输入以下命令：

```
dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /g
CONTOSO\JaneDoe:LCRP
```

在此示例中，已经为用户 CONTOSO\JaneDoe 授予对树枝的 《列出内容》和 《读属性》许可权限。这些许可权限足以让用户查看 Deleted Objects 树枝的内容。但是，这些许可权限不允许用户对该树枝中的对象执行任何更改。这些许可权限等效于授予给 Administrators 组的默认许可权限。默认情况下，只有 System 帐户有权修改 Deleted Objects 树枝中的对象。

应显示以下输出：

```
      Owner: CONTOSO\Domain Admins Group: NT AUTHORITY\SYSTEM
Access list: {This object is protected from inheriting permissions
from the parent} Allow BUILTIN\Administrators  SPECIAL ACCESS LIST
CONTENTS READ PROPERTY Allow NT AUTHORITY\SYSTEM     SPECIAL ACCESS
DELETE READ PERMISSONS WRITE PERMISSIONS CHANGE OWNERSHIP CREATE
CHILD DELETE CHILD LIST CONTENTS WRITE SELF WRITE PROPERTY READ
PROPERTY Allow CONTOSO\JaneDoe        SPECIAL ACCESS LIST CONTENTS
READ PROPERTY The command completed successfully.
```

现在，用户 CONTOSO\JaneDoe 有权查看 CONTOSO 域中的已删除对象。